Hindawi
Complexity
Volume 2020, Article ID 5725842, 11 pages
https://doi.org/10.1155/2020/5725842

Research Article

A Real-Time Image Encryption Method of Networked Inverted Pendulum Visual Servo Control System

Xue Li, Bing Liu, and Changda Zhang

School of Mechatronical Engineering and Automation, Shanghai University, Shanghai, China

Correspondence should be addressed to Xue Li; lixue@i.shu.edu.cn and Bing Liu; liu3371472@shu.edu.cn

Received 14 April 2020; Accepted 19 May 2020; Published 8 June 2020

Guest Editor: Zhile Yang

In the real-time control of networked inverted pendulum visual servo control system (NIPVSCS), how to achieve safe and efficient image transmission is an important and challenging problem. Generally, the inverted pendulum images are directly transmitted via the network, while these images are not secure because they may be attacked by the hacker. To solve the problem, a fast image encryption method by combining image scaling and improved self-diffusion image encryption (ISDIE) algorithm is firstly proposed, which is employed to encrypt the captured images after they are scaled. The security performance of the proposed algorithm, the characteristics of different delays, and the control performance of the NIPVSCS are then analyzed. Finally, simulation and real-time control experiments confirm the feasibility and effectiveness of the proposed method.

1. Introduction

Networked inverted pendulum system is a typical experimental platform to verify control theory and algorithms in the automatic control field [1–4]. In the recent years, with the rapid development of visual technique, visual sensors (e.g., the industrial camera) are gradually integrated into industrial control systems for detection and control [5–8]. To provide theoretical and technical support for visual servo real-time control, networked inverted pendulum visual servo control system (NIPVSCS) has been constructed and real-time H_∞ control method has also been proposed [9].

The network brings convenience to the transmission of visual images; however, these images also face various cyber attacks. In the NIPVSCSs, there exist not only the attacks on visual images but also the attacks on nonvision information. Here, this paper focuses on the security of the images because the attack on the image will reduce the image reliability (i.e., integrity and authenticity) and then cause the inaccurate and incomplete state and control information [9, 10], leading to system performance degradation or even instability.

To improve the security of the image, the image encryption provides a possible path. However, unlike the nonreal-time image encryption (e.g., the image encryption algorithms for health information exchange and enterprise remote audit), the image must be encrypted and decrypted quickly to guarantee the stable operation of the NIPVSCS. Therefore, the current image encryption algorithms cannot be employed directly, and the novel image encryption algorithms need to be developed in term of two requirements: (1) the processing speed of the image encryption and decryption algorithms must be very fast and (2) the image encryption and decryption algorithms must be robustness against the attacks.

To solve the abovementioned problems, this paper proposes a fast image encryption method of the NIPVSCS. The main contributions include

(1) A fast encryption method by combining the image scaling and an ISDIE algorithm is proposed to achieve secure and efficient transmission of the images.

(2) The security performance of the proposed algorithm, the characteristics of different delays, and the control performance of the NIPVSCS are analyzed. Simulation and real-time control experiments show that the proposed method has good encryption and

decryption effects and good robustness against the image noise attacks and shear attacks, while meeting real-time requirements of the NIPVSCS.

2. Related Work

The previous works on the NIPVSCS and the image encryption will be reviewed, and the unique features of this paper are discussed.

2.1. Real-Time Control of the NIPVSCS. The NIPVSCS is the system where the images of the inverted pendulum are captured by visual sensors and the images are then transmitted to the image processing unit via the network, followed by the state information extracted from these images. The obtained state information is then used to achieve real-time control, which is attached to delay constraints including network-induced delay and image processing computational delay. Furthermore, some methods are proposed to overcome these two delays. For example, the finite-time H_∞ stability analysis of uncertain network-based control systems under varying network delay was studied [11]. The stability analysis of the NCSs with the fixed time delay was discussed [12], and a new approach to the sub-optimal control of nonlinear time-delay systems was presented [13]. In [14, 15], the time-varying delay and image processing computational delay are considered, and a closed-loop control system model is established and H_∞ control strategy is used to achieve the stable of the control system. However, the abovementioned studies did not consider the image security (e.g., the leakage or corruption of information). In the NIPVSCS, since the state information is included in the images, it is crucial to protect these images.

In this paper, an NIPVSCS equipped with an image encryption unit is proposed to address the problem of image security. The control performance of the NIPVSCS is also analyzed under cyber attacks.

2.2. Image Encryption Algorithm. The image encryption algorithms, a common technique for image security, are usually used to protect image information from illegal acquisition. Recently, some image encryption algorithms have been developed. For example, according to the DNA encryption algorithm and the double-chaotic system, an image encryption-then-transmission system was presented [16]. An encryption method based on interleaved computer-generated holograms displayed by a spatial light modulator was proposed [17]. A hybrid image encryption scheme based on block compressive sensing was developed [18]. The image was encrypted by adopting the image encryption algorithm based on logistic map [19, 20]. However, the above proposed approaches induce the long encryption calculation delay that cannot meet the real-time requirements of the NIPVSCS.

In this paper, a fast image encryption method is developed to improve the security of the image and achieve real-time control of the NIPVSCS. The process of the fast image encryption method by combining image scaling and the ISDIE algorithm is provided and its security is then analyzed by simulation and real-time experiments.

3. The Proposed Framework

An image scaling and encryption unit is added to the pre-established NIPVSCS [21]. Figure 1 outlines the system framework that contains two parts: Part 1 is the NIPVSCS; Part 2 is the proposed fast encryption method combining image scaling and the ISDIE algorithm.

3.1. Part 1: The NIPVSCS. As can be seen from the left part of Figure 1, the NIPVSCS consists of the inverted pendulum (containing a cart, a swing rod, and a slide), the visual sensing devices (containing Aca640-120 gm industrial camera and a light source), the image scaling and encryption unit, the controller (containing a motion control card), and the actuator (containing servo driver and servo motor).

The operation of the NIPVSCS starts from the move of the swing rod. The real-time moving image of the inverted pendulum captured by the industrial camera is sent to the image scaling and encryption unit. In this unit, as shown in the right part of Figure 1, the inverted pendulum image is firstly scaled to reduce the amount of the image data, and the scaled image is then encrypted with an ISDIE algorithm to ensure image transmission security. Moreover, it can be seen from the right part of Figure 1 that the pixel values of each row of the image are confused to obtain a row confusing image, and the pixel values of each column of the image are confused to obtain a column confusing image, by implementing image encryption. Returning to the left part of Figure 1, the encrypted image is sent to the remote image processing unit through a network. In the remote image processing unit, the encrypted image is decrypted, and the state information of the cart and the pendulum is then extracted by using a series of image processing methods [22–25], which will be sent to the controller. Finally, the actuator processes the corresponding control signals to achieve real-time stable control of the NIPVSCS.

Remark 1. Different from most previous research studies only verified in simulations, the new NIPVSCS is based on a real experimental platform that can be used to validate the theoretical methods. Moreover, compared with the NIPVSCS in [21], two new units are added into the new NIPVSCS, i.e., the image scaling and encryption unit and the remote image processing unit.

3.2. Part 2: The Fast Image Encrytion Method

3.2.1. Image Scaling. Due to the large amount of inverted pendulum image data, long delays will be generated during network transmission and image encryption/decryption. To solve these problems, a method of interpolation scaling is used. Specifically, before the image is encrypted and transmitted, the inverted pendulum image is scaled down to reduce the amount of image data. This is shown in the right part of Figure 1. The image scaling can be expressed as the

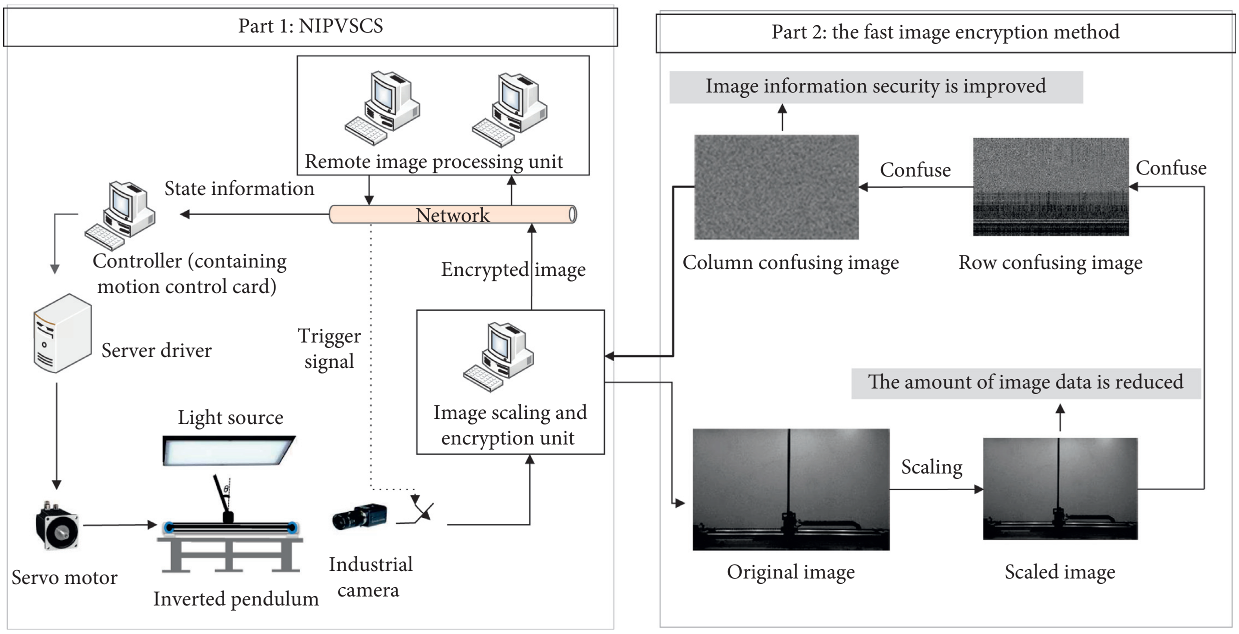


Figure 1: Framework of the NIPVSCS.

pixel position transformation followed by the calculation of pixel values, which will be given in the following.

(1) Pixel Position Transformation. Let $(srcx, srcy)$ and $(dstx, dsty)$ to be the pixel coordinates of the original inverted pendulum image and the scaled image, respectively. The formula of pixel position transformation is

$$\begin{aligned} dstx &= srcx * \frac{dstcols}{srccols}, \\ dsty &= srcy * \frac{dstrows}{srcrows}, \end{aligned} \tag{1}$$

where *srccols* and *dstcols* are the number of columns of the original image and the scaled image, respectively; *srcrows* and *dstrows* are the number of rows of the original image and the scaled image, respectively; and *dstcols/srccols* and *dstrows/srcrows* are the image scaling ratio in the horizontal direction and the vertical direction, respectively. The principle of scaling is shown in Figure 2.

Remark 2. To conveniently calculate the state information of the inverted pendulum in the scaled image, the equal scaling method is adopted, i.e., the same scaling ratio is taken in the horizontal and vertical directions, respectively.

Remark 3. To meet the real-time requirements of the NIPVSCS, we need to scale the image to a certain ratio before processing the inverted pendulum image to reduce the data amount of the original image. However, if the image scaling ratio is very small, it will lose a lot of image information, resulting in system performance degradation or even instability. Therefore, it is a trade-off between the image scaling ratio and system performance.

(2) Calculation of Pixel Values. To explain clearly, the gray values as a special case of the pixel values are concentrated. In Figure 2, the gray value of the coordinate (x, y) in the scaled image is that of the coordinate $(x + \Delta x, y + \Delta y)$ in the original image. However, since the coordinates of the pixel point are often integers and Δx and Δy could be nonintegers, the gray value of $(x + \Delta x, y + \Delta y)$ may not be directly obtained. Therefore, the bilinear interpolation method [26, 27] is used to calculate the gray value when the image is scaled, as shown in Figure 3.

In Figure 3, $f(x, y)$ represents the gray value of the coordinate (x, y). Two linear equations hold as follows:

$$\begin{aligned} f(x, y + \Delta y) = [&f(x, y + 1) - f(x, y)] \\ &* \Delta y + f(x, y), \end{aligned} \tag{2}$$

$$\begin{aligned} f(x + 1, y + \Delta y) = [&f(x + 1, y + 1) - f(x + 1, y)] \\ &* \Delta y + f(x + 1, y). \end{aligned} \tag{3}$$

Therefore, the gray value of $(x + \Delta x, y + \Delta y)$ can be calculated by

$$\begin{aligned} f(x + \Delta x, y + \Delta y) = &(1 - \Delta x)(1 - \Delta y) f(x, y + 1) \\ &- (1 - \Delta x)\Delta y f(x, y + 1) \\ &+ \Delta x (1 - \Delta y) f(x + 1, y) \\ &+ \Delta x \Delta y f(x + 1, y + 1). \end{aligned} \tag{4}$$

3.2.2. ISDIE Algorithm. The ISDIE algorithm includes two parts: the row confusion and column confusion. Before illustrating the ISDIE algorithm, $M \times N$ is the size of the inverted pendulum image, and $P_{i,j}$ is the pixel value at the ith row and jth column in the inverted pendulum image, where

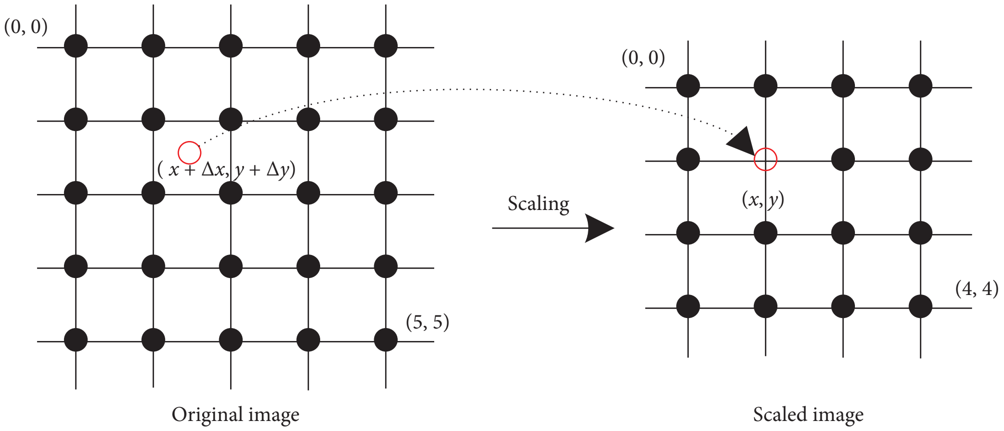


Figure 2: Schematic diagram of pixel position transformation.

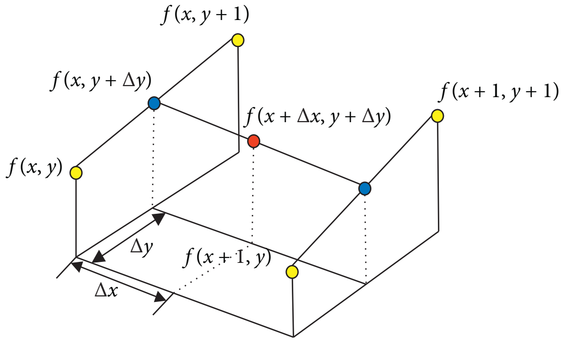


Figure 3: Schematic diagram of bilinear interpolation algorithm.

$1 \leq i \leq M$ and $1 \leq j \leq N$. In addition, we give the number t_k to the kth inverted pendulum image frame, where $t_k \geq k$. The ISDIE algorithm starts from the calculation of a regulation parameter T by using the number t_k of the kth inverted pendulum image frame.

Step 1: record the number of the each inverted pendulum image frame to obtain the regulation parameter T, and it is calculated by

$$T = \frac{\sum_{l=1}^{k} t_l}{1000}, \tag{5}$$

where the divisor is set as 1000.

The following are the procedures of row confusion and column confusion.

(1) Row confusion:

Step 2: to generate a pseudorandom state value as an encryption key, the logistic map [20, 21] is used as follows:

$$x_i = \mu x_{i-1} \left(1 - x_{i-1}\right), \tag{6}$$

where $x_i \in (0, 1)$ and $\mu \in (1, 4]$. In this paper, $x_0 = 0.19940730$ and $\mu = 3.999999$ are set to guarantee the randomness of the state value.

Step 3: then, x_i is used to generate other two different row numbers m and n by

$$m = \lceil x_i \times M \rceil, \tag{7}$$

$$n = \operatorname{mod}\left(\lfloor x_i \times 1000 \rfloor, M\right) + 1, \tag{8}$$

where $\lceil \cdot \rceil$ is the ceil function and $\lfloor \cdot \rfloor$ is the floor function and mod is a MOD function. To ensure that both m and n are different from i, the operations need to be further done as follows. (i) If $m = i$, $m = \operatorname{mod}(i, M) + 1$ will be done. (ii) If $n = i$, $n = \operatorname{mod}(i, M) + 1$ will be done.

Step 4: furthermore, m and n are used to confuse the current ith row by

$$P_{i,s} = P_{i,s} \oplus P_{m,s} \oplus P_{n,s}, \tag{9}$$

where $s = 1, \ldots, N$ and $\oplus$ is the boolean operator of *xor*.

Step 5: to achieve the "one time and one secret" of the encryption algorithm, the chaotic map value needs to be updated by

$$x_i = \left\{x_i + T\right\}, \tag{10}$$

where $\left\{x_i + T\right\}$ donates the decimal part of $x_i + T$.

Step 6: from the 1st row to the Nth row, the loop through Steps 2–6 to encrypt the inverted pendulum image in the row direction.

(2) Column confusion:

After the row confusion is completed, two changes on the procedure of row confusion can lead to that of column confusion: (i) change i as j in (6)–(8) and (10); (ii) then, change (9) as

$$P_{r,j} = P_{r,j} \oplus P_{r,m} \oplus P_{r,n}, \tag{11}$$

where $r = 1, \ldots, M$. Finally, the whole inverted pendulum image is encrypted in the row and column directions.

Remark 4. The traditional image encryption algorithms often take too long time to encrypt/decrypt the image so that the real-time requirement of the NIPVSCS could not be satisfied. In the context of the problem, by modifying the model of the image encryption algorithm in [21], the ISDIE algorithm is developed in this paper. To validate the efficiency of the ISDIE algorithm, the real-time experiments of the NIPVSCS running the above two algorithms are separately performed, whose results are shown in Table 1. From Table 1, it can be seen that the encryption time of the ISDIE algorithm is less than that of the algorithm in [21]. In this sense, the ISDIE algorithm is more suitable for the NIPVSCS. The experimental environment is Visual Studio 2010 and OpenCV2.4.11 with Intel Core i3-2120 CPU @ 3.30 GHz and 8.00 G RAM on Window XP.

Table 1: Delay analysis of two different encryption algorithms.

Algorithm	Ref. [21]	ISDIE
Encryption time	43 ms	15 ms

Remark 5. Considering the insecurity issues of the network (e.g., information loss and information disclosure), the serial number of the inverted pendulum images, which are unrelated to the contents of the image, are adopted to update the encryption key. Using this technology with different keys, the ISDIE algorithm can resist the plaintext-choosing attack and recover the core information when the encrypted images are corrupted by image noise attacks or shear attacks.

Furthermore, the ISDIE Algorithm 1 can be summarized as follows.

For the received encrypted image, decryption and encryption are inverse processes, and the decryption process is as follows.

(1) Column decryption:

Step 1: to generate a pseudorandom state value as an encryption key, the logistic maps are used as (6). To accurately decrypt the image, $x_0 = 0.19940730$ and $\mu = 3.999999$ are set to guarantee the randomness of the state value.

Step 2: create two auxiliary sequences and initialize them to 0, and the sequence is represented as follows:

$$J = [j_1, j_2, \ldots, j_N], \tag{12}$$

$$K = [k_1, k_2, \ldots, k_N]. \tag{13}$$

Step 3: fill the auxiliary sequence with

$$jj = \lceil x_j \times N \rceil, \tag{14}$$

$$kk = \lfloor x_j \times 1000 \rfloor \operatorname{mod} N + 1, \tag{15}$$

if $jj = j$, then $jj = j \operatorname{mod} N + 1$ and if $kk = j$, then $kk = i\operatorname{mod} N + 1$. Furthermore, $j_j = jj$ and $k_j = kk$.

Step 4: to achieve the "one time and one secret" of the encryption algorithm, the chaotic map value needs to be updated by

$$x_j = \left\{x_j + T\right\}, \tag{16}$$

where $\{x_j + T\}$ denotes the decimal part of $x_j + T$ and the value of T is the same as the value of T in Step 1.

Step 5: from column 1 to column N, the loop steps 1–4 to fill the auxiliary sequence.

Step 6: set $j = N$ and decrypted image by

$$P_{i,j} = P_{i,j} \oplus P_{i,j_j} \oplus P_{i,k_j}, \tag{17}$$

where $i = 1, \ldots, M$.

Step 7: from the Nth column to the 1st column, the loop through Step 6 decrypts the inverted pendulum image in the column direction.

(2) Row decryption

After the column decryption is completed, two changes on the procedure of columns decryption can lead to that of rows decryption: (i) change j as i in (12)–(16); (ii) then, change (17) as

$$P_{i,j} = P_{i,j} \oplus P_{j_i,j} \oplus P_{k_i,j}, \tag{18}$$

where $j = 1, \ldots, N$. Finally, the whole inverted pendulum image is decrypted in the row and column directions.

4. Experiments Analysis

4.1. Security Analysis of the ISDIE Algorithm. The security of the ISDIE algorithm mainly involves two aspects, i.e., key confidentiality and image robustness. The former strives for the attackers unavailable to the original key. The latter focuses on the decryption robustness against the attacks. The detailed analysis is discussed as below.

4.1.1. Analysis of Key Confidentiality. In the context of key confidentiality, three types of common attacks are considered. The first is the brute-force attacks, which attempts to traverse all possible keys for the intercepted ciphertext. The second, which can be viewed as an improvement of the first, adopts the statistical methods to obtain the distribution characteristics of the ciphertext so that the amount of searching messages or keys is reduced. Going further than both the above attacks, the plaintext is used for the comparison with the ciphertext in the third type of the attack.

(1) Brute-Force Attacks. To cope with brute-force attacks, the key used to encrypt the inverted pendulum image requires a sufficiently large key space and high sensitivity to key changes. In this paper, a test is carried out to prove that the

```
Input: The original inverted pendulum image
Output: The encrypted image
$l \longleftarrow 1$ to $k$ with the stepsize of 1 do $T \longleftarrow \mathrm{mod}(\sum_{l=1}^{k} t_l, 1000)$
  For $i \longleftarrow 1$ to $M$ with the stepsize of 1 do
    $x_i \longleftarrow \mu x_{i-1}(1 - x_{i-1})$, $m \longleftarrow \lceil x_i \times M \rceil$, $n \longleftarrow \mathrm{mod}(\lfloor x_i \times 1000 \rfloor, M) + 1$
    If $m = i$, $m \longleftarrow \mathrm{mod}(i, M) + 1$ end if
    If $n = i$, $n \longleftarrow \mathrm{mod}(i, M) + 1$ end if
    For $s \longleftarrow 1$ to $N$ with the stepsize of 1 do $P_{i,s} = P_{i,s} \oplus P_{m,s} \oplus P_{n,s}$ end for
    $x_i \longleftarrow \{x_i + T\}$
  End for
  For $j \longleftarrow 1$ to $N$ with the stepsize of 1 do
    $x_j = \mu x_{j-1}(1 - x_{j-1})$, $m = \lceil x_j \times N \rceil$, $n = \mathrm{mod}(\lfloor x_j \times 1000 \rfloor, N) + 1$
    If $m = i$, $m \longleftarrow \mathrm{mod}(i, M) + 1$ end if
    If $n = i$, $n \longleftarrow \mathrm{mod}(i, M) + 1$ end if
    For $r \longleftarrow 1$ to $M$ with the stepsize of 1 do $P_{r,j} = P_{r,j} \oplus P_{r,m} \oplus P_{r,n}$ end for
    $x_j \longleftarrow \{x_j + T\}$
  End for
```

ALGORITHM 1: ISDIE algorithm.

ISDIE algorithm can meet the above two requirements. In our test, three decrypted images using different keys infinitely close to the initial one are obtained in Figure 4. As can be seen in Figure 4, the key is hypersensitive in the decryption process and the key space of the encryption algorithm is more than 10^{56}. Therefore, the space is large enough to resist brute-force attacks.

(2) Statistical *Attacks*. To quantify the ability of coping with statistical attacks, the histogram of the images, the correlation of the pixels, and information entropy are adopted from different perspectives.

The histogram of the images is to describe the quality distribution characteristics [28]. The histograms of the original and encrypted images are shown in Figure 5. As can see from Figure 5(a), the gray-scale distribution of the original image is nonuniform and the characteristics peaks are clear. Conversely, the histogram of the encrypted image is uniform enough, as shown in Figure 5(b). This confirms the excellent property of resisting the statistical attack of the ISDIE algorithm.

The correlation of the pixels represents the randomness of the gray level. The correlation coefficients γ_{xy} of each pair can be calculated by

$$\mathrm{cov}(x, y) = E\{(x - E(x))(y - E(y))\},$$
$$\gamma_{xy} = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{19}$$

where x and y denote the values of two adjacent pixels in the image:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i, D(x) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)\right)^2, \tag{20}$$

where N denotes the number of pairs of adjacent pixels.

The correlation of the encrypted and original image is shown in Figure 6 and Table 2. The correlation of the original is high and close to 1. In contrast, the correlation of the encrypted image is low and close to 0, which indicates that encrypted pixels are distributed randomly.

Information entropy is used to reflect the randomness and unpredictability of the image gray value. The inverted pendulum image is 256 gray level and the ideally result should be 8. If the information entropy is closer to 8, the randomness is better. Table 2 shows the information entropy at different image scaling ratios. From Table 2, it is known that entropies are close to 8, so the proposed algorithm has a good property of information entropy.

(3) Differential Attacks. Two indicators, the Number of Pixels Change Rate (NPCR) and the Unified Average Changing Intensity (UACI), are used to measure the ability of resisting differential attack. The ideal values of NPCR and UACI are 99.61% and 33.46%, respectively [16, 29], and the real result values of the ideal image encryption algorithm should be close to the ideal values. They can be calculated by

$$\mathrm{NPCR} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} D(i, j)}{M \times N} \times 100\%,$$
$$\mathrm{UACI} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\left(\left(\left|C_1(i, j) - C_2(i, j)\right|\right)/255\right)}{M \times N} \times 100\%, \tag{21}$$

where $C_1(i, j)$ and $C_2(i, j)$ denote the gray value of two images, D is a matrix, and when $C_1(i, j) = C_2(i, j)$, then $D(i, j) = 0$ or $D(i, j) = 1$, and M and N are the width and height of the inverted pendulum image, respectively.

To compare the performance, we randomly change the gray value of one pixel of the inverted plaintext image and repeat it 500 times. The NPCR and UACI are obtained, as shown in Figure 7, by the proposed algorithm, where it can be found that the proposed scheme can resist differential attack effectively.

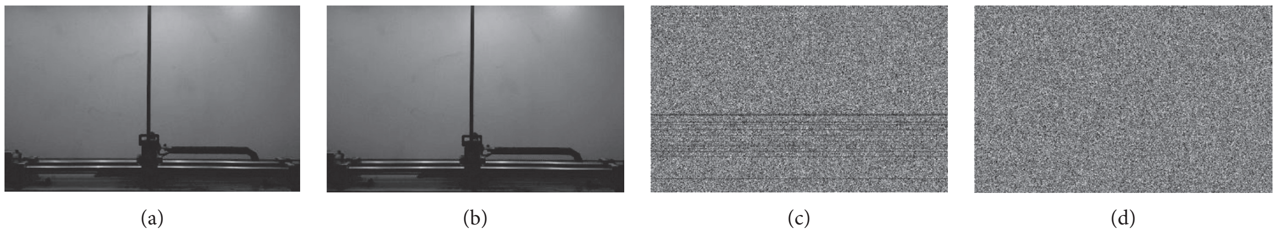


Figure 4: Key sensitivity analysis. (a) Original image. (b) Decrypted image: $x_0 = 0.19940730$ and $\mu = 3.999999$. (c) Decrypted image: $x_0 = 0.19940730 + 10^{-15}$ and $\mu = 3.999999$. (d) Decrypted image: $x_0 = 0.19940730$ and $\mu = 3.999999 + 10^{-15}$.

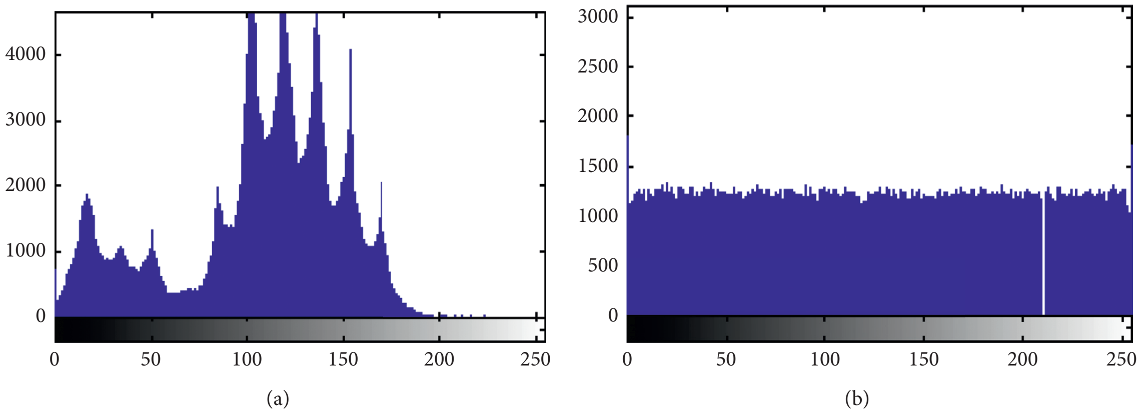


Figure 5: Histograms of the (a) original image and (b) encrypted images.

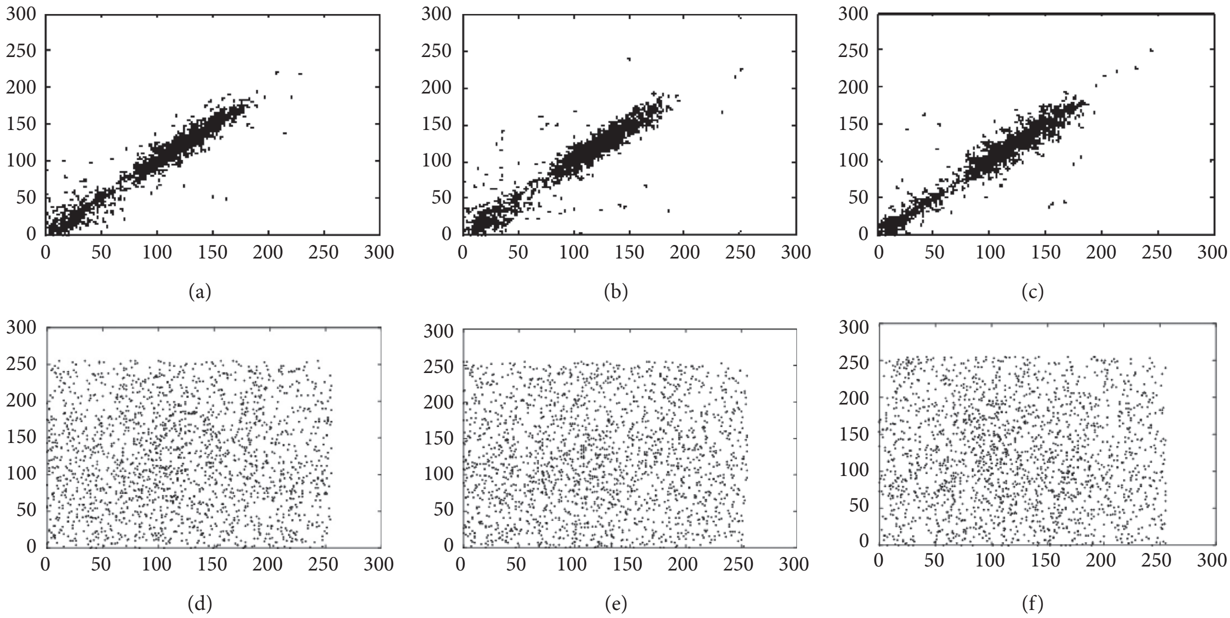


Figure 6: Correlation of two adjacent pixels (unscaled). (a) Vertical direction in the original image. (b) Horizontal direction in the original image. (c) Diagonal direction in the original image. (d) Diagonal direction in the encrypted image. (e) Horizontal direction in the encrypted image. (f) Diagonal direction in the encrypted image.

4.1.2. Analysis of Image Robustness. The above confirms the key confidentiality of ICDIE algorithm. Next, we will take into account the security issues about the disrupted image. Specifically, in the NIPVSCS, the images are vulnerable to the common image noise and shear attacks. Therefore, the image encryption algorithms for the NIPVSCS must be able

Table 2: Evaluation of encryption effect.

	Correlation of pixels			Information entropy
	Vertical	Diagonal	Horizontal	
Original image	0.9858	0.9240	0.9350	—
Encrypted image (unscaled)	0.0046	0.0047	0.0180	7.9843
Encrypted image (scaled ratio: 90%)	0.0056	0.0028	0.0296	7.9831
Encrypted image (scaled ratio: 70%)	−0.0025	0.0054	0.0312	7.9789
Encrypted image (scaled ratio: 50%)	0.0191	−0.0070	0.0406	7.9784
Encrypted image (scaled ratio: 40%)	−0.0433	−0.0090	0.0330	7.9779
Encrypted image (scaled ratio: 30%)	−0.0258	−0.0015	0.0157	7.9779

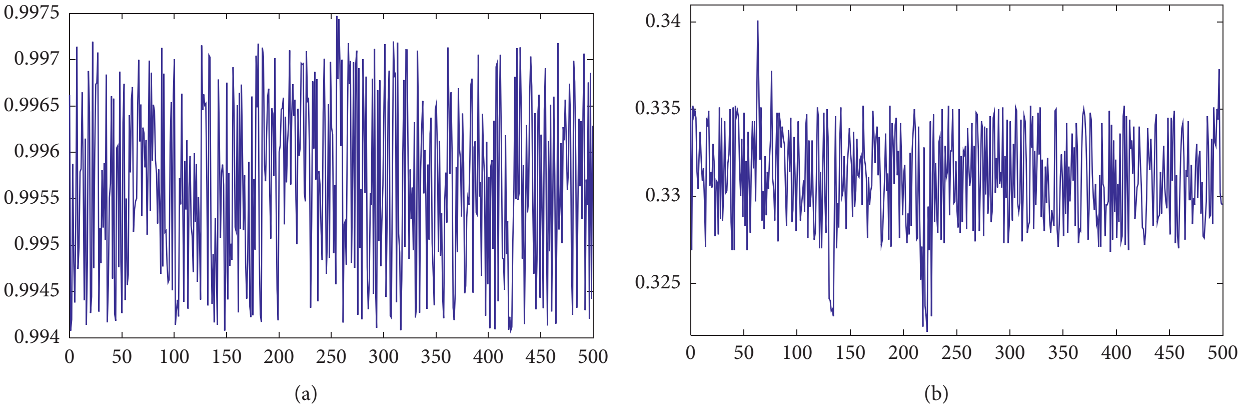


Figure 7: Only one pixel is changed by the (a) NPCR and (b) UACI, respectively.

to withstand common image attacks. To measure the robustness of the encryption algorithm against image attacks, some attack experiments on the ICDIE algorithm are conducted, and the corresponding decryption effect are analyzed. The results are shown in Figure 8.

4.2. Delay Analysis of the Proposed Fast Encryption Method Used in the NIPVSCS. In the NIPVSCS, the delay is a key factor affecting system stability [11]. In this paper, the NIPVSCS delays are mainly composed of network transmission delay, image encryption and decryption delay, and image processing computational delay. To analyze the delays of the NIPVSCS, real-time statistics on network transmission delay and image encryption and decryption computational delay under different image scaling ratios are firstly obtained, and then the total system delay in the NIPVSCS under different image scaling ratios is calculated.

4.2.1. Network Transmission Delay under Different Image Scaling Ratios. To obtain the network transmission delay, 2000 image frames are transmitted under different image scaling ratios in the NIPVSCS. The delay of each image frame is recorded and finally taken as an average. The results are shown in Table 3.

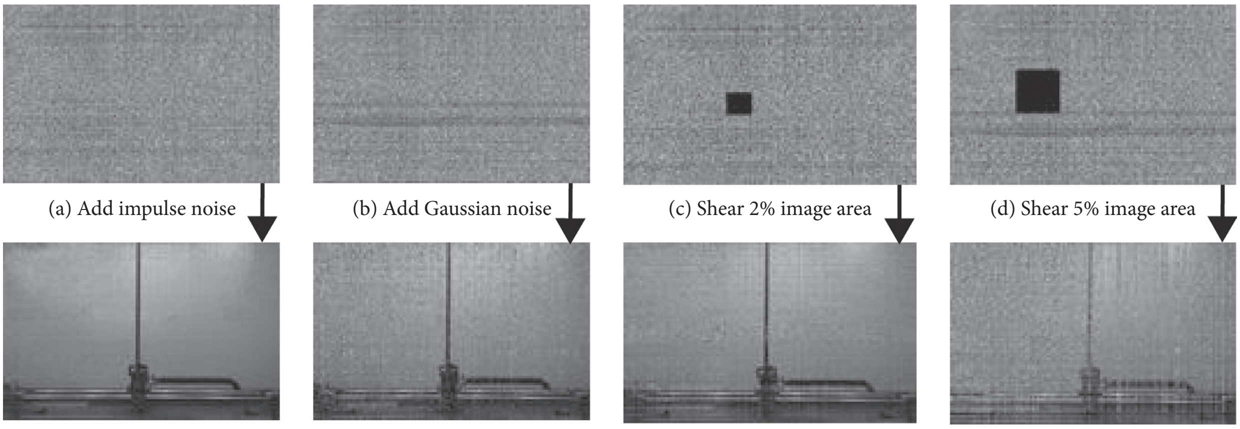
From Table 3, it can be seen that network transmission delay gradually decreases as the image scaling ratio decreases. This shows that scaling the inverted pendulum image can effectively reduce network transmission delay in the NIPVSCS.

4.2.2. Image Encryption and Decryption Delay under Different Image Scaling Ratios. The time of the inverted pendulum image encryption and decryption under different image scaling ratios is recorded in Figure 9. It can be seen that the encryption and decryption delay decreases as the image scaling ratio decreases.

4.2.3. Total System Delay under Different Image Scaling Ratios. We denote $d_k \in [\underline{d}, \overline{d}]$ by the total delay from the visual sensor to the controller, where $\underline{d}$ and $\overline{d}$ are, respectively, the lower and upper bounds of d_k. We record d_k under different image scaling ratios in Figure 10 and $\underline{d}$ and $\overline{d}$ in Table 4.

From Figure 10 and Table 4, it can be seen that the lower and upper bounds of the total delay decreases as the image scaling ratio decreases, respectively. In Table 4, $\overline{d}$ is lower than the real-time requirement of the NIPVSCS when the image scaling ratio is 30%, 40%, 50%, and 70%.

4.3. Secure Control Analysis of the Proposed Fast Encryption Method Used in the NIPVSCS. From [11, 14], it is known that the NIPVSCS will be unstable when the upper bound of the total delay is greater than or equal to 38 ms in real-time control environment. To analyze the feasibility of the



(a) Add impulse noise

(b) Add Gaussian noise

(c) Shear 2% image area

(d) Shear 5% image area

(e) Decrypted image

(f) Decrypted image

(g) Decrypted image

(h) Decrypted image

Figure 8: Robustness analysis of the ISDIE algorithm.

Table 3: Network transmission delay under different image scaling ratios.

Image scaling ratio	30%	40%	50%	70%	90%
Network transmission delay	4 ms	4 ms	6 ms	7 ms	10 ms

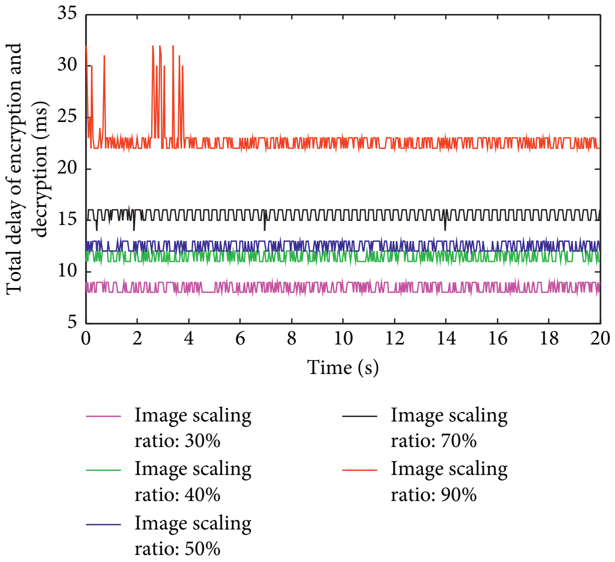


Figure 9: Encryption and decryption delay under different scaling ratios.

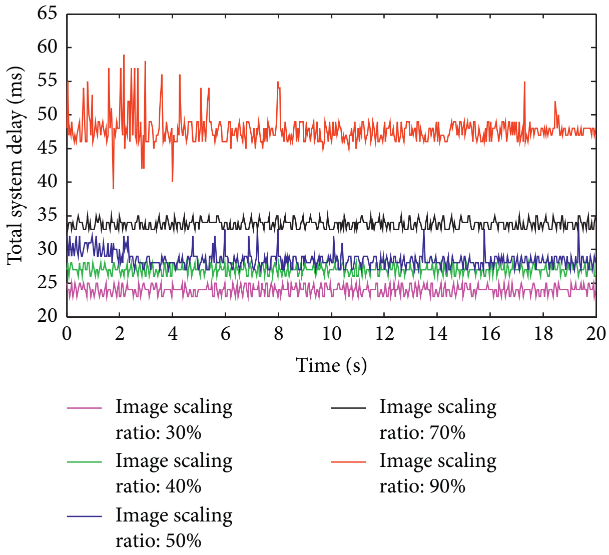


Figure 10: Total delay under different scaling ratios.

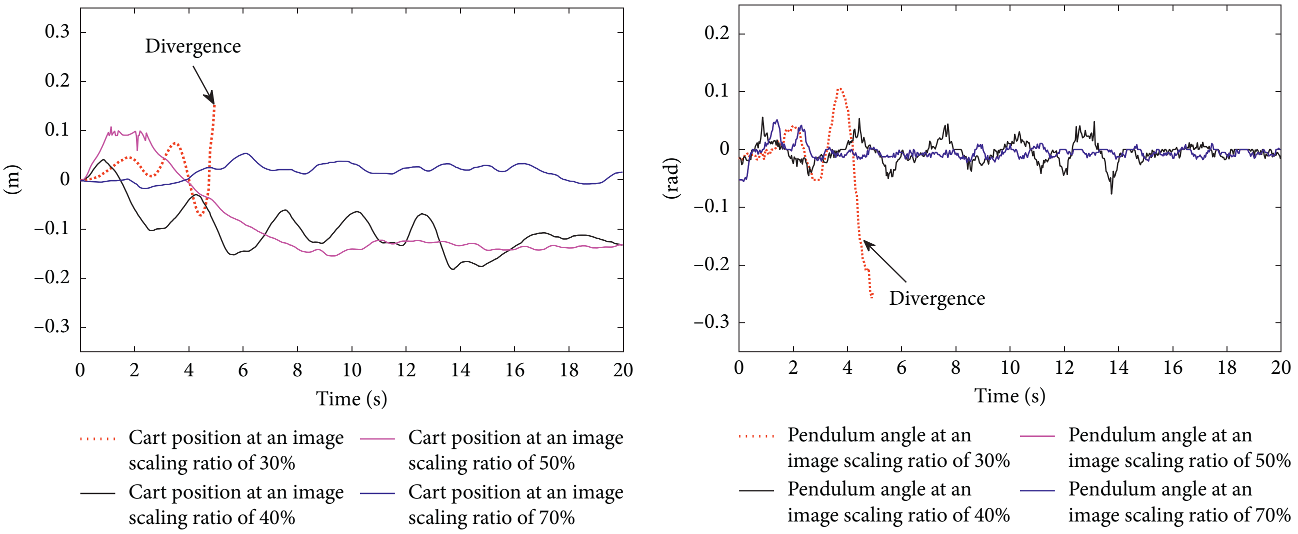
proposed fast encryption method in the NIPVSCS, the real-time control experiment is firstly carried out under no attack. The result is shown in Figure 11.

Figure 11 shows that the cart position and the pendulum angle fluctuate in a very small range when the image scaling ratio is 70%, 50%, and 40%, while the NIPVSCS is stable. However, the system control curve is diverging (i.e., the NIPVSCS is unstable) when the image scaling ratio is 30%. The distinction between the theoretical and real-time results may be caused by three aspects: (i) the difference of the linear model and nonlinear model of the plant; (ii) as the image scaling decreases, the image processing errors gradually increase; (iii) the unknown noise being overlooked. In the practical applications, a larger image scaling ratio should be selected to achieve real-time control when the delay requirements of system stability control are met.

Next, to verify the robustness of the ISDIE algorithm against image noise and shear attack, some real-time control experiments under the noise attack and shear attack are carried out, respectively. In this experiment, the image is scaled to 50%. The results are shown in Figure 12. As can be seen from Figure 12, the NIPVSCS can still remain stable even if the image is disrupted by image noise attacks. This

Table 4: The lower and upper bounds of the total system delay.

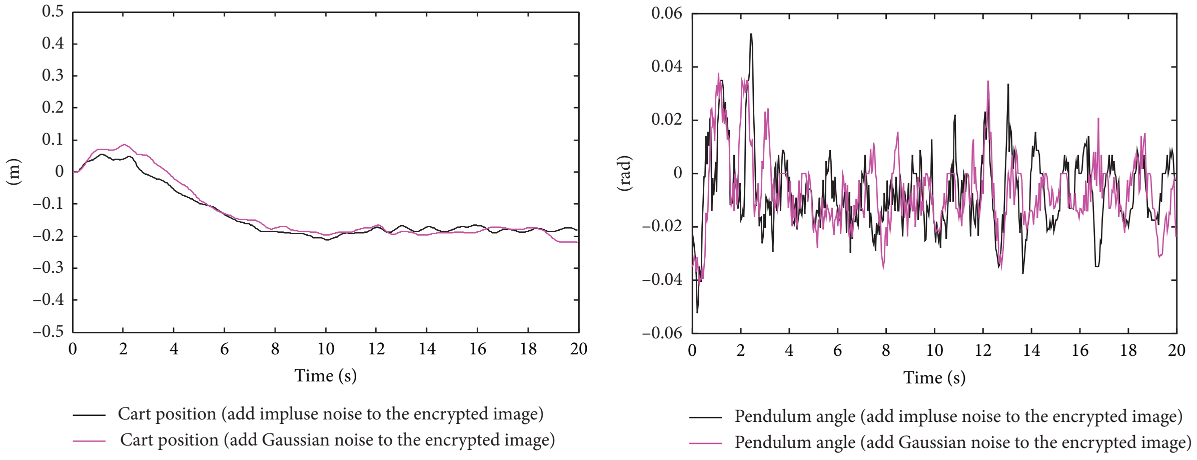
Scaling ratio	30%	40%	50%	70%	90%
$\underline{d}$	23 ms	25 ms	27 ms	33 ms	40 ms
$\overline{d}$	26 ms	28 ms	33 ms	35 ms	59 ms



(a)

(b)

Figure 11: Real-time control under different image scaling ratios (no attack).



(a)

(b)

Figure 12: Real-time control effect under different image scaling ratios (attacked).

shows the good robustness of the ISDIE algorithm against image noise attack NIPVSCS.

5. Conclusions

This paper addresses the problem of safe and efficient transmission of image in the NIPVSCS. Specifically, we have developed a fast encryption method combining image scaling and ISDIE algorithm, where the captured images are encrypted after they are scaled. We have evaluated our method by using the simulation and real-time experiments. The proposed method can guarantee the key confidentiality and image robustness and meet the real-time control requirements of the NIPVSCS with some certain image scaling ratio. However, the scaled inverted pendulum image will reduce image quality to some extent and cause image processing errors. Therefore, considering the effect of image processing error caused by image scaling on the stability of the NIPVSCS is a very valuable future work. Moreover, the fast encryption method can be successfully used for a fast motion control system, i.e., NIPVSCS security and stability control, which can further provide technical support for remote vision robot control, aircraft control, and other applications.

Data Availability

The experimental data used to support the findings of this study have not been made available since these data are related to the personal privacy of each volunteer involved in the experiment.

Conflicts of Interest

The authors declare that there are no conflicts of interest.

Acknowledgments

This work was supported in part by the National Science Foundation of China (Grant nos. 61773253 and 61833011) and Key Project of Science and Technology Commission of Shanghai Municipality (Grant no. 16010500300).

References

[1] C. S. Chen and W. L. Chen, "Robust adaptive sliding-mode control using fuzzy modeling for an inverted-pendulum system," *IEEE Transactions on Industrial Electronics*, vol. 45, no. 2, pp. 297–306, 1998.

[2] S. Kim and S. Kwon, "Nonlinear optimal control design for underactuated two-wheeled inverted pendulum mobile platform," *IEEE/ASME Transactions on Mechatronics*, vol. 22, no. 6, pp. 2803–2808, 2017.

[3] N. Muskinja and B. Tovornik, "Swinging up and stabilization of a real inverted pendulum," *IEEE Transactions on Industrial Electronics*, vol. 53, no. 2, pp. 631–639, 2006.

[4] D. Du, B. Qi, M. Fei, and Z. Wang, "Quantized control of distributed event-triggered networked control systems with hybrid wired-wireless networks communication constraints," *Information Sciences*, vol. 380, pp. 74–91, 2017.

[5] X. M. Zhang, Q. L. Han, X. Ge et al., "Networked control systems: a survey of trends and techniques," *IEEE/CAA Journal of Automatica Sinica*, vol. 7, no. 1, pp. 1–17, 2020.

[6] C. Wu, J. Liu, X. Jing, H. Li, and L. Wu, "Adaptive fuzzy control for nonlinear networked control systems," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 47, no. 8, pp. 2420–2430, 2017.

[7] N. Kottenstette, J. F. Hall, X. Koutsoukos, J. Sztipanovits, and P. Antsaklis, "Design of networked control systems using passivity," *IEEE Transactions on Control Systems Technology*, vol. 21, no. 3, pp. 649–665, 2013.

[8] J. Sztipanovits, B. Jia, and K. Zhang, "Trifocal tensor-based adaptive visual trajectory tracking control of mobile robots," *IEEE Transactions on Cybernetics*, vol. 47, no. 11, pp. 3784–3798, 2017.

[9] D. Du, C. Zhang, H. Wang, X. Li, H. Hu, and T. Yang, "Stability analysis of token-based wireless networked control systems under deception attacks," *Information Sciences*, vol. 459, pp. 168–182, 2018.

[10] T. Zseby, F. Iglesias Vazquez, A. King, and K. C. Claffy, "Teaching network security with IP darkspace data," *IEEE Transactions on Education*, vol. 59, no. 1, pp. 1–7, 2016.

[11] A. Claffy and A. Alfi, "Finite-time H_∞ stability analysis of uncertain network-based control systems under random packet dropout and varying network delay," *Nonlinear Dynamics*, vol. 91, no. 4, pp. 1–19, 2017.

[12] G. Wang, L. Li, and B. Wu, "Robust stability of nonlinear model-based networked control systems with time-varying transmission times," *Nonlinear Dynamics*, vol. 69, no. 3, pp. 1351–1363, 2012.

[13] M. Jamshidi, "A three-stage design of non-linear control systems with time-delay," *International Journal of Control*, vol. 21, no. 5, pp. 753–762, 1975.

[14] M. Y. Ma, B. L. Bai, and J. Y. Zou, "Improvement of congestion control for Ethernet communication in embedded visual system," *Computer Engineering and Application*, vol. 52, no. 9, pp. 116–121, 2016.

[15] J. Chen, S. Meng, and J. Sun, "Stability analysis of networked control systems with aperiodic sampling and time-varying delay," *IEEE Transactions on Cybernetics*, vol. 47, no. 8, pp. 2312–2320, 2017.

[16] X.-Q. Fu, B.-C. Liu, Y.-Y. Xie, W. Li, and Y. Liu, "Image encryption-then-transmission using DNA encryption algorithm and the double chaos," *IEEE Photonics Journal*, vol. 10, no. 3, pp. 1–15, 2018.

[17] D. Kong, L. Cao, X. Shen, H. Zhang, and G. Jin, "Image encryption based on interleaved computer-generated holograms," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 2, pp. 673–678, 2018.

[18] L. Zhu, H. Song, X. Zhang, M. Yan, L. Zhang, and T. Yan, "A novel image encryption scheme based on nonuniform sampling in block compressive sensing," *IEEE Access*, vol. 7, pp. 22161–22174, 2019.

[19] X. Wang, C. Liu, D. Xu, and C. Liu, "Image encryption scheme using chaos and simulated annealing algorithm," *Nonlinear Dynamics*, vol. 84, no. 3, pp. 1417–1429, 2016.

[20] X. Liu, Q. Wang, and Y. Zhang, "A fast image algorithm based on rows and columns switch," *Nonlinear Dynamics*, vol. 79, no. 2, pp. 1141–1149, 2015.

[21] D. Du, C. Zhang, Y. Song et al., "Real-time H_∞ control of networked inverted pendulum visual servo systems," *IEEE Transactions on Cybernetics*, pp. 1–14, 2019.

[22] D. V. Zhou, W. Goeman, P. Veelaert, and W. Philips, "Robust monocular visual odometry for road vehicles using uncertain perspective projection," *EURASIP Journal on Image & Video Processing*, vol. 2015, no. 1, p. 21, 2015.

[23] J. Canny, "A computational approach to edge detection," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 8, no. 6, pp. 679–698, 1986.

[24] M. E. Magana and F. Holzapfel, "Fuzzy-logic control of an inverted pendulum with vision feedback," *IEEE Transactions on Education*, vol. 41, no. 2, pp. 65–170, 1998.

[25] L. X. Liu and J. G. Liu, "Research on locating license plate's up and down edges," *Journal of Instrumentation*, vol. 26, no. 8, pp. 177–179, 2005.

[26] K. Arai, T. Kurihara, and K.-I. Anjyo, "Bilinear interpolation for facial expression and metamorphosis in real-time animation," *The Visual Computer*, vol. 12, no. 3, pp. 105–116, 1996.

[27] S. Wang and K. Z. Yang, "Research and implementation of image scaling algorithm based on bilinear interpolation," *Automation Technology and Applications*, vol. 27, no. 7, pp. 44-45, 2008.

[28] X. Y. Wang and H. L. Zhang, "A novel image encryption algorithm based on genetic recombination and hyper-chaotic systems," *Nonlinear Dynamics*, vol. 83, no. 83, pp. 333–346, 2016.

[29] Y. Li, C. Wang, and H. Chen, "A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation," *Optics and Lasers in Engineering*, vol. 90, pp. 238–246, 2017.