Secure Control of Networked Inverted Pendulum Visual Servo System with Adverse Effects of Image Computation

Dajun Du, Changda Zhang, Qianjiang Lu, Minrui Fei, and Huiyu Zhou

***Abstract*—When visual image information is transmitted via communication networks, it easily suffers from image attacks, leading to system performance degradation or even crash. This paper investigates secure control of networked inverted pendulum visual servo system (NIPVSS) with adverse effects of image computation. Firstly, the image security limitation of the traditional NIPVSS is revealed, where its stability will be destroyed by eavesdropping-based image attacks. Then, a new NIPVSS with the fast scaled-selective image encryption (F2SIE) algorithm is proposed, which not only meets the real-time requirement by reducing the computational complexity, but also improve the security by reducing the probability of valuable information being compromised by eavesdropping-based image attacks. Secondly, adverse effects of the F2SIE algorithm and image attacks are analysed, which will produce extra computational delay and errors. Then, a closed-loop uncertain time-delay model of the new NIPVSS is established, and a robust controller is designed to guarantee system asymptotic stability. Finally, experimental results of the new NIPVSS demonstrate the feasibility and effectiveness of the proposed method.**

***Index Terms*—Networked visual servo system, image encryption, parameter uncertainty, time delay, robust controller.**

I. Introduction

Networked visual servo control [1] has been a class of new control system technology along with rapid development of visual sensors (e.g., camera [2] and radar [3]) and communication network. It has been gradually employed in some innovative scenarios such as autonomous vehicles, mobile robots, unmanned helicopter and intelligent manufacturing. However, it also brings some new problems (e.g., long image processing time, non-ignorable image computational error and potential image attacks), which will lead to system performance degradation or even crash. To solve these new problems, some new control methods and technologies of networked visual servo control needs to be developed, which also needs further be validated on proper experimental platforms. The traditional inverted pendulum system [4], [5] is a typical experimental platform, but it cannot directly work for validation. It must be reformed, which is reconstructed as networked inverted pendulum visual servo system (NIPVSS) [6], [7].

Communication networks are introduced into NIPVSS, where the system becomes open to the public. It will inevitably suffer from cyber attacks [8] such as false data injection attacks and denial-of-service attacks, which causes the system to be deteriorate or crash. The current research mainly focuses on non-visual information under cyber attacks. However, when visual image information is transmitted via communication networks, it suffers from eavesdropping-based image attacks such as salt and pepper attack, shearing attack, Gaussian attack. These images attacks tamper with the information after eavesdropping the images, which will further make the receiver be unable to obtain the correct and integral image information, leading to system performance degradation and even instability. Thus, how to guarantee the image security during network transmission is a critical issue. To achieve the image security, the most popular method is chaotic image encryption. For example, an image encryption method is proposed by combining dynamic DNA sequence encryption and hyper-chaotic maps [9]; A colour image encryption algorithm with higher security based on the chaotic system is proposed to ensure safe transmission of image information [10]. These chaotic image encryption methods are mainly employed to encrypt non-real-time images, which do not consider real-time requirements in industrial control applications.

Image attacks will bring extra computational errors, while the image encryption methods will produce extra computational delay, further declining system performance. However, the most existing NIPVSS do not consider the image attacks and not consider computational delay or errors either [11]. But there exists several studies that begin to consider the impact of errors on the inverted pendulum system (IPS). For example, the influence of pendulum angle errors on the IPS is considered [12] and the errors are taken as an energy finite disturbance and H_∞ controller is designed to suppress this disturbance [7]. Besides the error problems, the delay related to the networked control system has been reported. For instance, a new controller based on sliding mode estimation is designed to handle the time delay system with different input matrices [13]; Based on a new event triggering mechanism, T-S fuzzy event triggering control is employed to support the distributed delay system [14]; Stabilization of time-delay systems under delay-dependent impulse control is studied [15].

The work of Dajun Du, Changda Zhang, Qianjiang Lu and Minrui Fei was supported in part by the National Science Foundation of China under Grant 92067106, Grant 61633016, Grant 61773253, Grant 61803252, and Grant 61833011; in part by the 111 Project under Grant D18003; and in part by the Project of Science and Technology Commission of Shanghai Municipality under Grant 20JC1414000, Grant 19500712300, Grant 19510750300, and Grant 21190780300.

Dajun Du, Changda Zhang, Qianjiang Lu and Minrui Fei are with Shanghai Key Laboratory of Power Station Automation Technology, School of Mechatronic Engineering and Automation, Shanghai University, Shanghai 200444, China (e-mail: ddj@i.shu.edu.cn; lqj18490@shu.edu.cn; changdazhang@shu.edu.cn; mrfei@staff.shu.edu.cn).

Huiyu Zhou is with School of Computing and Mathematical Sciences, University of Leicester, Leicester LE1 7RH, U.K (e-mail: hz143@leicester.ac.uk).

Preprint submitted to IEEE Transactions on Control Systems Technology. Received: September 10, 2023 20:55:06 Pacific Time

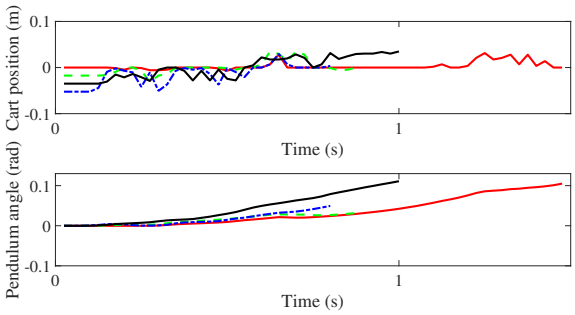


Fig. 1. Cart position and pendulum angle of traditional NIPVSS under shearing attacks with different shearing rates: —, 1% shearing rate; - -, 2% shearing rate; · · · · ·, 4% shearing rate; —, 5% shearing rate.

Furthermore, the image attacks (e.g., shearing attacks) are operated for the most existing NIPVSS, experimental results of Fig. 1 shows that traditional NIPVSS runs for a short time and then collapses. This is because some areas of images are cut off intentionally so that accurate system state cannot be obtained. Therefore, based on these observations, we have analysed two challenge problems that need to be addressed:

1) What is the image security limitation of the traditional NIPVSS? How to establish a new NIPVSS with image encryption to not only meet the real-time requirement but also guarantee image security?
2) What are adverse effects of image information security? How to build a closed-loop model under the adverse effects and design a robust controller with strong system stability to tolerate computational errors and delays?

To deal with these challenges, this paper investigates secure control of NIPVSS with adverse effects of image computation. Comparative analysis between contributions of this paper and those of existing image encryption and control methods is shown in Tab. I. Some existing advanced image encryption algorithms mainly solve security problems of still images but usually have high computational complexity, and some other existing references on NIPVSS mainly provide controller design methods and stability criteria under network and image processing computation constraints but cannot consider image attacks. In this paper, we have revealed image security limitation of traditional NIPVSS, proposed a fast image encryption algorithm to meet real-time requirement, established a new model including extra computational delay and errors produced by image encryption and image attacks, and designed a new robust controller to guarantee system stability. The main contributions of this paper include:

1) The image security limitation of traditional NIPVSS is revealed, where its stability will be destroyed by eavesdropping-based image attacks. To overcome the limitation, a new NIPVSS with a fast scale-selective image encryption (F2SIE) algorithm is proposed, which not only meets real-time requirement by reducing computational complexity, but also improves security of new NIPVSS by reducing probability of valuable information being compromised by eavesdropping-based image attacks.
2) Adverse effects of the F2SIE algorithm and image attacks are analysed, which will produce extra computational delay and extra computational errors. A closed-loop uncertain time-delay model of the new NIPVSS is then established, and a robust controller is designed to guarantee system asymptotic stability.

TABLE I
COMPARATIVE ANALYSIS BETWEEN THIS PAPER AND EXISTING REFERENCES

References	IAE[1]	RR[2]	CD[3]	CE[4]	ND[5]	ECD[6]	ECE[7]
[9], [10]	✔	✗	✗	✗	✗	✔	✗
[11]	✗	✗	✗	✗	✗	✗	✗
[12]	✗	✗	✗	✔	✗	✗	✗
[7]	✗	✗	✔	✔	✔	✗	✗
[13]–[15]	✗	✗	✗	✗	✔	✗	✗
This paper	✔	✔	✔	✔	✔	✔	✔

[1]Image attack and image encryption. [2]Real-time requirement for image encryption.[3]Computational delay from image processing. [4]Computational error from image processing. [5]Network-induced delay from network transmission. [6]Extra computational delay from image encryption. [7]Extra computational error from image attack.

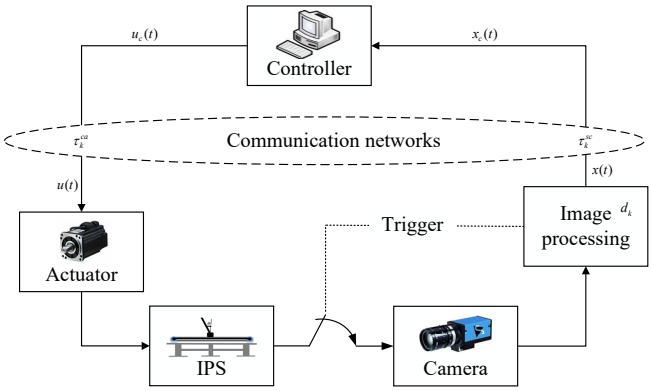


Fig. 2. The structure of traditional NIPVSS [7].

The remainder of this paper is organized as follows. In Section II, the image security limitation of traditional NIPVSS is firstly analysed, and new NIPVSS with an F2SIE algorithm is then proposed. In Section III, adverse effects caused by F2SIE algorithm and image attacks are analysed and thus a new closed-loop NIPVSS model is established. Furthermore, the control design of new NIPVSS with F2SIE algorithm is presented . Section IV presents experimental results. Conclusions and future work are given in Section V.

II. THE TRADITIONAL AND NEW NIPVSS

A. Image Security Limitation of the Traditional NIPVSS

The structure of traditional NIPVSS [7] is shown in Fig. 2, where real-time moving images of IPS captured by industrial cameras based on an event-triggered sampling strategy are sent to image processing unit to extract system state, and the acquired system state is sent to remote controller for calculating control input. Finally, the corresponding control input is sent to actuator for achieving stable control of IPS.

In view of both communication and computational constraints in Fig. 2, an H_∞ controller $u_c(t) = Kx(t)$ is designed

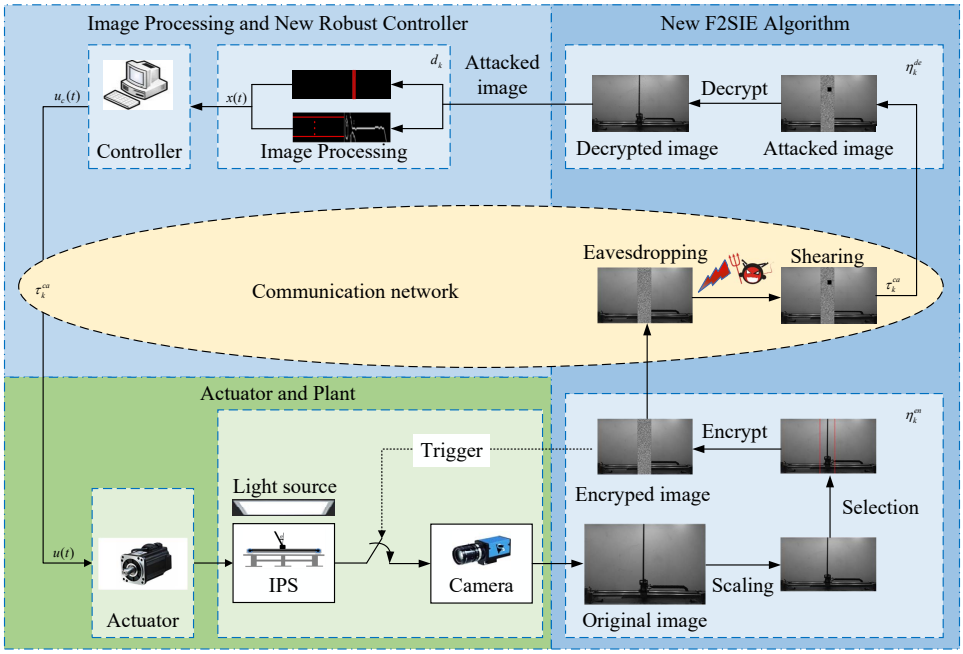


Fig. 3. The structure of the new NIPVSS combined with the proposed F2SIE algorithm and robust controller. An example of the new NIPVSS under a slight eavesdropping-based shearing attack (e.g., with shearing rate 1%) is shown. In this case, the image decrypted by the F2SIE algorithm will be with small errors. This indicates that the F2SIE algorithm can improve security of the new NIPVSS against eavesdropping-based image attacks.

to achieve system stability in [7] where K is feedback gain. The closed-loop model of traditional NIPVSS is

$$\begin{cases} \dot{x}(t) = Ax(t) + BKx(t - d(t) - \tau(t)) + B_\omega \omega(t), \\ t \in [t_k + d_k + \tau_k^{sc} + \tau_k^{ca}, t_{k+1} + d_{k+1} + \tau_{k+1}^{sc} + \tau_{k+1}^{ca}), \end{cases} \tag{1}$$

where $x(t) = [\alpha(t), \theta(t), \dot{\alpha}(t), \dot{\theta}(t)]$ is system state, $\alpha(t)$, $\theta(t)$, $\dot{\alpha}(t)$ and $\dot{\theta}(t)$ are cart position, pendulum angle, cart and angular velocity respectively; $d(t)$ is image-induced delay; $\tau(t)$ is network-induced delay; t_k is image sampling instant; d_k is image processing time; τ_k^{sc} is network transmission time from sensor to controller; τ_k^{ca} is network transmission time from controller to actuator; $B_\omega \omega(t)$ is computational errors; A and B are constant matrices.

In the above traditional NIPVSS, images may be attacked in an open network, which will lead to system performance degradation or even crash (see an example of Fig. 1).

B. The New NIPVSS with an F2SIE algorithm

To cope with the above problem of image attacks, a fast scaled-selective image encryption (F2SIE) algorithm will be proposed, which can ensure image security while meet real-time requirement. The structure of new NIPVSS with F2SIE algorithm is shown in Fig. 3. The difference between Figs. 2 and 3 lies on that the image is encrypted at the local end and the corresponding image via network transmission is decrypted at the remote end so as to guarantee image security. After decryption, the system state are obtained and then sent to controller. Furthermore, the control input is calculated in terms of system state, which is finally transmitted to actuator via network and to make IPS run stably.

The idea of F2SIE algorithm is that image is scaled and the scaled image is then encrypted by replacement and diffusion. The encryption steps are as follows:

1) **Image scaling and selection:** To reduce image transmission and encryption time, a bilinear difference method is employed to scale original image of IPS (e.g., 40%), maintaining continuity of the generated pixel value to ensure image smooth. To further reduce amount of image data, Hough transform is used to determine position of pendulum and the width is set as 100 pixels to cover cart and pendulum. The final selected area is shown in Fig. 4 of [16].
2) **Generation of initial values:** After image scaling and selection, next task is to encrypt key areas, Bülban mapping is used to generate random numbers as follows

$$y_{n+1} = y_n \times \sqrt{\frac{a}{y_n - b}}, \tag{2}$$

where a and b are artificially selected parameters, respectively. The chaotic system (2) is a one-dimensional chaotic system, which can effectively reduce generation time in comparison with complex chaotic systems. Fig. 5 of [16] shows Bifurcation and Lyapunov indexes analysis of Bülban mapping when $a = 0.5$ and $b = 2$, where it can be seen that system has a large chaotic range with few or no non-chaotic window. The size of the encrypted area is P, where $P_i (i \in \{1, 2, \cdots, M\})$ and $P_j (j \in \{1, 2, \cdots, N\})$ represent rows and columns of the encrypted area respectively. Bülban mapping operates 500 times with initial value y_0 to ensure its chaos.
3) **Replacement algorithm:** After chaotic system parameters is set, they can be used to generate random numbers

for replacement and diffusion. Bülban mapping is used to generate two real number sequences $PR = \{PR_i\}$ and $PC = \{PC_j\}$ where $i \in \{1, 2, \cdots, M\}$, $j \in \{1, 2, \cdots, N\}$. Then, real number sequences PR and PC are converted into unsigned integer number sequences

$$PR^{un} = \{PR_i^{un} | PR_i^{un} = PR_i \times 10^5 \bmod M\} \quad (3)$$
$$PC^{un} = \{PC_j^{un} | PC_j^{un} = PC_j \times 10^5 \bmod N\}. \quad (4)$$

PR^{un} corresponds to each row in P, and the pixel values of each row in P are cyclically shifted according to PR^{un} so that P becomes P^{sr}, i.e.,

$$P_{ij}^{sr} = \begin{cases} P_{i,j-PR_j^{un}}, if\ j > PR_j^{un} \\ P_{i,j+N-PR_j^{un} \bmod N}, if\ j \leqslant PR_j^{un} \end{cases} \quad (5)$$

Similarly, PC^{un} corresponds to each column in P^{sr}, and the pixel values of each row in P^{sr} are cyclically shifted based on PC^{un} so that P^{sr} becomes P^{sc}, i.e.,

$$P_{ij}^{sc} = \begin{cases} P_{i-PC_i^{un},j}^{sr}, if\ i > PC_i^{un} \\ P_{i+M-PC_i^{un} \bmod M,j}^{sr}, if\ i \leqslant PC_i^{un} \end{cases} \quad (6)$$

An example is shown in Fig. 6 of [16].

4) **Diffusion algorithm:** After replacement, it is necessary to change pixel value to improve encryption. Bülban mapping is used to generate real sequence $\mathcal{K} = \{\mathcal{K}_{ij}\}$, where $i \in \{1, 2, \cdots, M\}$ and $j \in \{1, 2, \cdots, N\}$. Then, $\mathcal{K}$ is converted into unsigned integer number sequence

$$\mathcal{K}^{un} = \left\{\mathcal{K}_{ij}^{un} | \mathcal{K}_{ij}^{un} = \mathcal{K}_{ij} \times 10^5 \bmod 256\right\}. \quad (7)$$

To improve security of encryption algorithm, the ciphertext feedback mechanism is integrated into diffusion stage, which is shown in Fig. 7 of [16], while the bidirectional ciphertext feedback mode is employed to avoid feedback effect of the first or the last pixel from one-way feedback mechanism. P^{sc} with positive feedback is denoted as $P^{po} = \{P_{ij}^{po}\}$, and P^{po} with negative feedback is denoted as $P^{ne} = \{P_{ij}^{ne}\}$. P^{po} and P^{ne} can be described by

$$P_{ij}^{po} = \begin{cases} (P_{00}^{sc} \otimes \mathcal{K}_{00}^{un} + \mathcal{K}_{00}^{un}) \bmod 256, if\ i = 0, j = 0; \\ (P_{ij}^{sc} \otimes \mathcal{K}_{ij}^{un} + \mathcal{K}_{i-1,N}^{un}) \bmod 256 \otimes P_{i-1,N}^{sc}, \\ if\ i \neq 0, j = 0; \\ (P_{ij}^{sc} \otimes \mathcal{K}_{ij}^{un} + \mathcal{K}_{i,j-1}^{un}) \bmod 256 \otimes P_{i,j-1}^{sc}, \\ if\ i = 0, j \neq 0. \end{cases} \quad (8)$$

$$P_{ij}^{ne} = \begin{cases} (P_{MN}^{po} \otimes \mathcal{K}_{MN}^{un} + \mathcal{K}_{MM}^{un}) \bmod 256, \\ if\ i = M, j = N; \\ (P_{ij}^{po} \otimes \mathcal{K}_{ij}^{un} + \mathcal{K}_{i+1,0}^{un}) \bmod 256 \otimes P_{i+1,0}^{po}, \\ if\ i \neq M, j = N; \\ (P_{ij}^{po} \otimes \mathcal{K}_{ij}^{un} + \mathcal{K}_{i,j+1}^{un}) \bmod 256 \otimes P_{i,j+1}^{po}, \\ if\ i = M, j \neq N. \end{cases} \quad (9)$$

The whole image encryption process is summarized in Algorithm 1 of [16], while the decryption process is a reverse process of the encryption so it is omitted.

The new NIPVSS with F2SIE algorithm has been proposed, which not only improves security of new NIPVSS by reducing probability of valuable information being compromised by eavesdropping-based image attacks, but also meets real-time requirement by reducing computational complexity. Therefore, the challenge 1 is solved.

Remark 1: The F2SIE algorithm is used to improve security of new NIPVSS against eavesdropping-based image attacks. Take shearing attack as an example. When F2SIE algorithm is not used, shearing attacks can shear valuable information (e.g., a part of the pendulum) from the eavesdropped unencrypted image with probability 1, so that pendulum angle cannot be obtained and NIPVSS will lose its stability. When there exists F2SIE algorithm, valuable information is uniformly distributed in image [17] (see an example in Fig. 8 of [16]). For simplicity, consider a case where image is with $\mathcal{N}_i \in \mathbb{Z}_+$ pixels and the sheared area is with $\mathcal{N}_s \in \mathbb{Z}_+$ pixels. In this case, the probability that the sheared area of the eavesdropped encrypted image contains all valuable information (e.g., a part of pendulum) is $1/\mathcal{C}_{\mathcal{N}_i}^{\mathcal{N}_s}$ due to uniformly distributed characteristics of the encrypted image, where $\mathcal{C}$ is combination number. Even if $\mathcal{N}_i$ is small (e.g., $\mathcal{N}_i = 100$), when shearing rate is small (e.g., 4% that is $\mathcal{N}_s = 0.04 \times \mathcal{N}_i = 4$), the probability $1/\mathcal{C}_{\mathcal{N}_i}^{\mathcal{N}_s}$ is very small ($1/\mathcal{C}_{\mathcal{N}_i}^{\mathcal{N}_s} = 2.6034 \times 10^{-7}$). Therefore, the decrypted image under shearing attacks with small shearing rates will have small error with the unencrypted image. It has been verified in real-world experiments of Section IV that cart position and pendulum angle can be obtained with small errors under eavesdropping-based image attacks and the proposed controller hereinafter can be used to stabilize new NIPVSS.

Remark 2: Compared with existing advanced image encryption methods (e.g., [18], [19]) with high computational complexity, F2SIE algorithm is with low computational complexity. Specifically, for encryption of an $M \times N$ ($M \in \mathbb{Z}_+$, $N \in \mathbb{Z}_+$) image, F2SIE algorithm only needs $O(MN + M + N)$ iterations of floating point numbers multiplication, while [18] and [19] need $O(3MN)$ and $O(2MN)$ iterations. Moreover, in real-world experiments, it is verified that for encryption and decryption of an 100×480 image, F2SIE algorithm consumes $0.014s$, while [18] and [19] consume $0.021s$ and $0.019s$. Therefore, existing advanced image encryption methods in [18], [19] cannot meet real-time requirement of new NIPVSS (i.e., they cannot work in new NIPVSS), but F2SIE algorithm can meet high real-time requirement of new NIPVSS.

Remark 3: In real-world industrial applications, the (private or public) key used for encryption and decryption can be fixed [20] or random [21], however random key is more difficult to be decrypted and thus provides better security than fixed key. Furthermore, the usage of random private key in F2SIE algorithm requires that encryption and decryption device keep synchronization, which can be implemented by key synchronization algorithm [22]. The detailed process of key synchronization algorithm is as follows: The key used in F2SIE algorithm is firstly from chaotic sequences. Then, when initial value and parameters in (2) are the same, encryption and decryption device can generate two identical chaotic sequences. Next, according to the agreed choosing order (e.g., choosing from the 100-th number in chaotic sequence),

encryption and decryption device can keep same key from the same chaotic sequences. Therefore, the synchronization of random ley can be guaranteed.

Remark 4: When images are severely compromised by image attacks (e.g., shearing attacks with big shearing rates) in new NIPVSS, some new techniques such as authentication [23] and signature [24] need to be adopted to prevent from information leakage. In the worst case after the above techniques are invalid, attack detection and data compensation [25] can be used to improve system security.

III. Adverse Effects Analysis and Robust Controller Design

A. Adverse Effects of F2SIE Algorithm and Image Attacks

The above has designed a new NIPVSS with F2SIE algorithm to guarantee image security. However, this will bring some adverse effects, i.e., extra computational times from F2SI2 algorithm and extra computational errors from image attacks. It will degrade system performance or even drive system collapse. For instance, Fig. 9 of [16] shows experimental results of new NIPVSS with F2SIE algorithm under the H_∞ controller in [7], where new NIPVSS is unstable after the images have been encrypted and decrypted. Hence, these adverse effects must be analysed.

1) Extra Computational Times from F2SIE Algorithm: There already exist $\tau_k^{sc} \in [\underline{\tau}^{sc}, \bar{\tau}^{sc}] = [0, 0.005s]$, $\tau_k^{ca} \in [\underline{\tau}^{ca}, \bar{\tau}^{ca}] = [0, 0.005s]$ and $d_k \in [\underline{d}, \bar{d}] = [0.009s, 0.019s]$ in traditional NIPVSS [7]. After F2SIE algorithm is introduced, its consumed time cannot be ignored, which cause system unstable as shown in Fig. 9 of [16]. Therefore, two extra computational times are to be analysed, i.e., image encryption time η_k^{en} and image decryption time η_k^{de}. From experimental statistical results in Section III.A of [16], their upper and lower bounds are $\eta_k^{en} \in [\underline{\eta}^{en}, \bar{\eta}^{en}] = [0.004, 0.007]s$ and $\eta_k^{de} \in [\underline{\eta}^{de}, \bar{\eta}^{de}] = [0.004, 0.007]s$.

Remark 5: To meet high real-time requirement of new NIPVSS, image scaling and selection are adopted in F2SIE algorithm to reduce delay. Therefore, original image processing time $d_k \in [0.009, 0.019]s$ in [7] is reduced to scaled-selective image processing time $d_k \in [0.007, 0.009]s$ in this paper.

Remark 6: When image attacks begin to enter new NIPVSS, they require a certain injection time $\Delta\eta_k$ to modify the encrypted pixel. The values of $\Delta\eta_k$ of different image attacks are shown in Tab. II of [16], where it can be seen that: $\Delta\eta_k$ of slight shearing attack and salt and pepper attack is almost zero, and only 0.001s with increase of attack intensity; $\Delta\eta_k$ of Gaussian attack is generally 0.001s. Therefore, $\Delta\eta_k$ is treated as a constant, i.e., $\Delta\eta_k = \Delta\eta = 0.001s$. Although injection time of these attacks is short, it must be considered when designing a robust controller.

2) Extra Computational Errors from Image Attacks: The F2SIE algorithm brings extra computational delay, but does not cause extra computational errors. This is because encryption process is completely opposite to decryption process so that image can be decrypted with zero errors. However, it has been analysed in [7] that environmental noise will cause computational errors. Moreover, attacks on the encrypted images will produce extra computational errors. These computational errors will destroy system stability, which is well illustrated in Fig. 1.

The computational errors from environmental noise and image attacks need be converted into form of parameter uncertainty, where conversion process is shown in Section III.A of [16]. The final conversion result is

$$\Delta A = DF(t)E, \tag{10}$$

where $\Delta A = diag\{\Delta_1 + \Delta_{1,a}, \Delta_2 + \Delta_{2,a}, 0, 0\}$ is the whole parameter uncertainty matrix, $\Delta_1 \in [-0.4, 0.4]$ and $\Delta_2 \in [-0.82, 0.82]$ are parameter uncertainty of cart position and pendulum angle caused by environmental noise respectively, $\Delta_{1,a} \in [\underline{\Delta}_{1,a}, \overline{\Delta}_{1,a}]$ and $\Delta_{2,a} \in [\underline{\Delta}_{2,a}, \overline{\Delta}_{2\_a}]$ are parameter uncertainty of cart position and pendulum angle caused by image attacks respectively; $D = I$; $F(t) = diag\{r_1(t), r_2(t), 0, 0\}$, $r_1(t) \in [-1, 1]$, $r_2(t) \in [-1, 1]$; $E = diag\left\{0.4 + \Delta_{1,a}^M, 0.82 + \Delta_{2,a}^M, 0, 0\right\}$, $\Delta_{1,a}^M = max\left\{|\underline{\Delta}_{1,a}|, |\overline{\Delta}_{1,a}|\right\}$ and $\Delta_{2,a}^M = max\left\{|\underline{\Delta}_{2,a}|, |\overline{\Delta}_{2,a}|\right\}$.

Remark 7: When no attack, both $\Delta_{1,a}$ and $\Delta_{2,a}$ are zero. When the encrypted images are attacked, $\Delta_{1,a}$ and $\Delta_{2,a}$ from image attacks are added into Δ_1 and Δ_2 from environmental noise, leading to system performance decrease or even crash.

B. Closed-Loop Uncertain Model of New NIPVSS

The adverse effects (i.e., extra computational times and extra computational errors) from F2SIE algorithm and image attacks in new NIPVSS have been analysed. Next, to design a new robust controller $u_c(t) = Kx(t)$, the closed-loop model of new NIPVSS with F2SIE algorithm under image attacks need to be established. The detailed modelling process can be seen in Section III.B of [16], and finally a new closed-loop NIPVSS model with parameter uncertainty and multiple time-varying delays can be established as

$$\begin{cases} \dot{x}(t) = (A + DF(t)E)x(t) + BKx(t - \lambda(t) - \tau(t)), \\ t \in \left[t_k + \eta_k^{en} + \Delta\eta_k + \tau_k^{sc} + \eta_k^{de} + d_k + \tau_k^{ca}, \right. \\ \left. t_{k+1} + \eta_{k+1}^{en} + \Delta\eta_{k+1} + \tau_{k+1}^{sc} + \eta_{k+1}^{de} + d_{k+1} + \tau_{k+1}^{ca}\right), \end{cases} \tag{11}$$

where $\tau(t) \in [0, \bar{\tau}]$ is network-induced delay and $\bar{\tau} = \bar{\tau}^{ca}$; $\lambda(t) \in [\underline{\lambda}, \bar{\lambda}]$ is the new image-induced delay, $\underline{\lambda} = \underline{\eta}^{en} + \Delta\eta + \underline{\tau}^{sc} + \underline{\eta}^{de} + \underline{d}$ and $\bar{\lambda} = 2\bar{\eta}^{en} + 2\Delta\eta + \bar{\tau}^{sc} + \bar{\eta}^{de} + \bar{d}$.

Remark 8: The problem of network communication and image processing has been well handled in [7], but problem of image attacks is not involved. The image attacks can degrade system performance or even cause system crash. To cope with image attacks, new F2SIE algorithm has been designed in the above. However, F2SIE algorithm brings some new problems that the controller in [7] with F2SIE algorithm cannot keep system stable as shown in experimental results of Fig. 9 of [16]. To solve these problems, a new closed-loop uncertain time-delay model (11) has been established, including that 1) extra computational delays in $\lambda(t)$ caused by F2SIE algorithm running time η_k^{en}, η_k^{de} and image attacks injection time $\Delta\eta_k$ are considered in (11), 2) extra computational errors caused by image attacks are considered, and the whole computational errors caused by environment noise and image attacks are treated

as parameter uncertainty $DF(t)E$ in (11). In comparison with time-delay model (1) in [7], the controller in [7] is invalid and a new robust controller must be designed for new model (11).

C. Robust Controller Design

As a typical networked visual servo control application scenario, new NIPVSS with F2SIE algorithm under image attacks has been established as the above closed-loop model (11), which is regarded as an uncertain time-delay system. For this system, it can be handled based on the idea of robust networked control [7], [26], [27], and a new robust controller is designed in the following Theorem 1.

Theorem 1: For given constants $0 < \overline{\tau}$, $0 < \underline{\lambda} < \overline{\lambda}$, $0 < \varepsilon_1$, $0 < \varepsilon_2$ and $\theta_j (j = 1, 2, 3, 4)$, if there exist $0 < \epsilon$ and real symmetric matrices X, $\tilde{Q}_i$ $(i = 1, 2, \cdots, 7)$, $\tilde{Z}_i$ $(i = 1, 2, 3, 4)$ with appropriate dimensions, such that

$$\begin{bmatrix} \Phi_{11} & \Phi_{12} & \Phi_{13} \\ * & \Phi_{22} & 0 \\ * & * & -\epsilon I \end{bmatrix} < 0, \tag{12}$$

holds, where Φ_{11}, Φ_{12}, Φ_{13}, Φ_{22} are given in Section III.C of [16], then the closed-loop system (11) with gain $K = YX^{-1}$ is asymptotically stable for parametric uncertainty satisfying $\|F(t)\| \leqslant 1$ and time delays in (11).

Proof: The proof is given in Section III.C of [16]. ■

Remark 9: Adverse effects of F2SIE algorithm and image attacks have been analysed, which will produce extra computational delay and extra computational errors. According to these adverse effects, a new closed-loop uncertain time-delay model (11) of new NIPVSS is established. For (11), an error-as-parameter-uncertainty robust controller is designed by Theorem 1, which can achieve system asymptotic stability. Specially, unlike [7], new robust controller can handle the following two cases: 1) When uncertainty ranges of cart position and pendulum angle under image attacks are within $0.4+\Delta_{1,a}^{M}$, $0.82 + \Delta_{2,a}^{M}$, the controller is robust to parameter uncertainty from computational errors, i.e., system remains stability; 2) When $\tau(t)$, $\lambda(t)$ are within $[0, \bar{\tau}]$, $[\underline{\lambda}, \bar{\lambda}]$, the controller is robust to these two delays partly from image encryption and decryption, i.e., system is still stable. Therefore, the challenge 2 is solved.

IV. Experimental Results and Discussion

To verify the proposed F2SIE algorithm and robust controller, real-time control experiments are carried out, where new NIPVSS platform based on [28] is shown in Fig. 4.

A. Performance of F2SIE Algorithm

The performance of F2SIE algorithm will be analysed by six aspects, where two aspects (algorithm running time and image robustness) are analysed in the following and the other four aspects are analysed in Section IV.A of [16]. The analysis results are summarized in Tab. III of [16]. The real-time performance of encryption is firstly analysed, because only when real-time performance is satisfied, system can run stably.

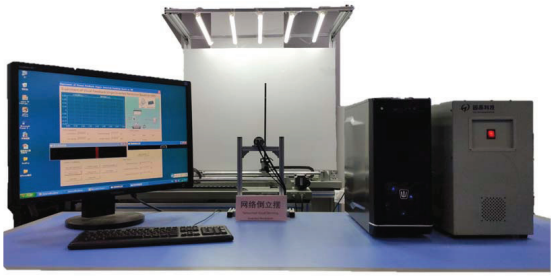


Fig. 4. Experimental platform of new NIPVSS fused with the proposed F2SIE algorithm and robust controller.

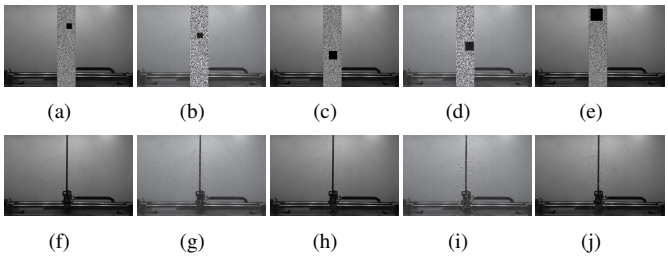


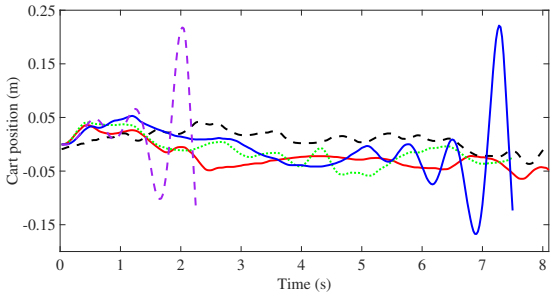
Fig. 5. (a)-(e): The encrypted images under shearing attacks with different shear rates (1%, 2%, 4%, 5%, 6%). (f)-(j): The decrypted images of (a)-(e).

1) Algorithm Running Time: Real-time performance is one of key factors for stable operation of NIPVSS, where image scaling and selection in F2SIE algorithm can reduce amount of image data. Moreover, F2SIE algorithm reduces encryption time by generating row-column-level random numbers for encryption. The second row of Tab. III of [16] shows running time of different algorithms, where it can be seen that F2SIE algorithm meets real-time requirement in comparison with [29].

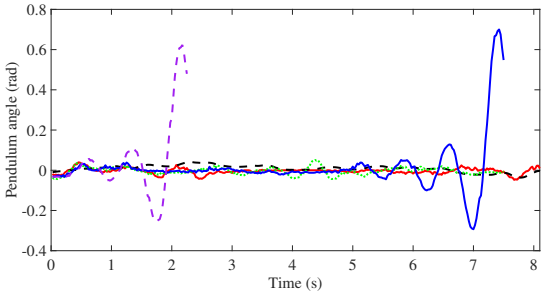
2) Image Robustness: It is a common phenomenon that image is often subject to shearing, salt and pepper or Gaussian attacks during network transmission. For new NIPVSS, image decryption will be affected by these image attacks. Peak signal-to-noise ratio (PSNR) is an objective standard [30], and generally when PSNR is lower than 20dB, image quality is poor to unacceptable and feature extraction cannot be performed. Tab. IV of [16] shows PSNR of the decrypted IPS image under these image attacks, where it can be seen that the stronger image attacks are, the lower PSRN are. But PSNR are all more than 20dB, which indicates that F2SIE algorithm has ability to keep image under these image attacks with good quality. Meanwhile, Fig. 5 (slight shearing attacks) and Figs. 16 (slight salt and pepper attack) and 17 (slight Gaussian attack) of [16] shows that F2SIE algorithm can recover effective information of pendulum and cart after being affected by these slight image attacks. However, when attack is added too much, the recovered image contour will gradually become blurred.

B. Controller Robustness

The proposed F2SIE algorithm has been confirmed, then controller robustness will be analysed. Using Theorem 1, some parameters are given as $\underline{\eta}^{en} = 0.004s$, $\bar{\eta}^{en} = 0.007s$, $\underline{\eta}^{de} =$

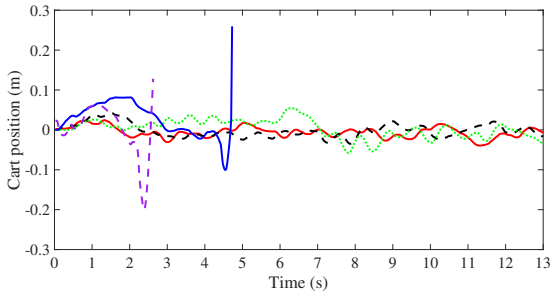


(a) Cart position

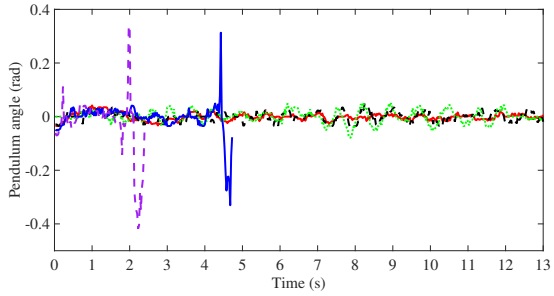


(b) Pendulum angle

Fig. 6. Cart position and pendulum angle of the new NIPVSS with different upper bounds $\bar{\eta}^{en}+\bar{\eta}^{de}$ of image encryption and decryption time: —, $\bar{\eta}^{en}+\bar{\eta}^{de}=0.014s$; - -, $\bar{\eta}^{en}+\bar{\eta}^{de}=0.015s$; · · · · ·, $\bar{\eta}^{en}+\bar{\eta}^{de}=0.016s$, —, $\bar{\eta}^{en}+\bar{\eta}^{de}=0.017s$; - -, $\bar{\eta}^{en}+\bar{\eta}^{de}=0.018s$.



(a) Cart position



(b) Pendulum angle

Fig. 7. Cart position and pendulum angle of the new NIPVSS under shearing attacks with different shearing rates: — represents 1% shearing rate, - - represents 2% shearing rate, · · · · · represents 4% shearing rate, — represents 5% shearing rate and - - represents 6% shearing rate.

$0.004s$, $\bar{\eta}^{de}=0.007s$, $\bar{\tau}=0.005s$, $\underline{\lambda}=0.026s$, $\bar{\lambda}=0.054s$, $\theta_1=0.01$, $\theta_2=0.75$, $\theta_3=1.2$, $\theta_4=0.022$, $\varepsilon_1=0.9$, $\varepsilon_2=0.1$, $\Delta_{1,a}=\Delta_{2,a}=0$. Before image is encrypted, each image has an exposure time of 0.01s. Thus, an additional 0.01s is needed for all parameters involved in image encryption. Using the above parameters and solving (12), control gain K of closed-loop system (11) can be calculated, and its value is $K=[3.7633,-29.9925,4.0355,-5.4562]$

The controller robustness will be analysed from two aspects.

1) Controller Robustness against Multiple Delay: The relationship between $\tau(t)$ and $\lambda(t)$ is firstly analysed. By using Theorem 1, theoretical $\bar{\tau}$ and $\bar{\lambda}$ can be obtained while closed-loop system (11) is stable. Tab. V of [16] lists this relationship between $\bar{\tau}$ and $\bar{\lambda}$, where theoretical $\bar{\tau}$ is from $0s$ to $0.013s$, and the corresponding theoretical $\bar{\lambda}$ is from $0.067s$ to $0.054s$. To analyse impact of image encryption-decryption time $\eta_k^{en}+\eta_k^{de}$ on the system, value of $\bar{\eta}^{en}+\bar{\eta}^{de}$ is calculated. Recalling $\bar{\lambda}=2\bar{\eta}^{en}+\bar{\eta}^{de}+\bar{\tau}^{sc}+\bar{d}$ with fixed $\bar{\tau}^{sc}$ and $\bar{d}$, the corresponding values of $\bar{\eta}^{en}+\bar{\eta}^{de}$ can be calculated ($\bar{\eta}^{en}=\bar{\eta}^{de}$), which is shown in the third row of Tab. V of [16]. For instance, when $\bar{\tau}=0.005s$, the theoretical $\bar{\eta}^{en}+\bar{\eta}^{de}$ is 0.018s.

To further explore the maximum experimental value of $\bar{\eta}^{en}+\bar{\eta}^{de}$ that system can tolerate when $\bar{\tau}=0.005s$, values of $\bar{\eta}^{en}+\bar{\eta}^{de}$ are set as 0.014s, 0.015s, 0.016s, 0.017s, 0.018s. Real-time curves of cart position and pendulum angle are shown in Fig. 6, where is can be seen that as $\bar{\eta}^{en}+\bar{\eta}^{de}$ increases, the fluctuation of cart position and pendulum angle increases. When $\bar{\eta}^{en}+\bar{\eta}^{de}$ goes to $0.017s$ or $0.018s$, cart position and pendulum angle diverge. Hence, when $\bar{\tau}=0.005s$, the maximum experimental value of $\bar{\eta}^{en}+\bar{\eta}^{de}$ that system can tolerate is $0.016s$.

2) Controller Robustness against Parameter Uncertainty: The relationship between Δ_1 and Δ_2 is analysed. According to Theorem 1, for the given $|\Delta_1|$, $|\Delta_2|$ can be obtained while ensures closed-loop system (11) stable, where $|\Delta_1|$ is from 0 to 0.67 and the corresponding $|\Delta_2|$ is from 3.24 to 0. Furthermore, to analyse $\Delta_{1,a}$ and $\Delta_{2,a}$ caused by image attacks, we add shearing attack, salt and pepper attack and Gaussian attack in images. The analysis for salt and pepper attack and Gaussian attack are given in Section IV.B of [16]. The following is analysis for shearing attack.

Different shearing rates (1.0%, 2.0%, 4.0%, 5.0%) of shearing attacks are added, and the corresponding real-time curves of cart position and pendulum angle are shown in Fig. 7. It can be seen from Fig. 7 that when shearing rate is within 4.0%, cart position and pendulum angle tend to be stable and diverge when shearing rate exceeds 5.0%. However, when shearing rate goes to 5.0%, cart position and pendulum angle diverge rapidly. This is because information of the cut picture is seriously damaged, which leads to increase of computational error and makes system unstable. Hence, it means that the maximum shearing rate that system can withstand is 4.0%.

Values of $\underline{\Delta}_{1,a}$, $\underline{\Delta}_{2,a}$, $\overline{\Delta}_{1,a}$, $\overline{\Delta}_{2,a}$ under shearing attacks with different shearing rates are shown in Table II, where it can be seen that when IPS runs stably, $\Delta_{1,a}\in[-0.32,0.40]$ and $\Delta_{2,a}\in[-0.74,0.75]$. When IPS starts to diverge, $|\Delta_{1,a}|$ is beyond 0.45 and $|\Delta_{2,a}|$ is beyond 1.00. Hence, the designed controller can be able to achieve stable control of NIPVSS under slight shearing attacks, but cannot prevent from severe shearing attacks.

Preprint submitted to IEEE Transactions on Control Systems Technology. Received: September 10, 2023
20:55:06 Pacific Time

TABLE II
VALUES OF $\underline{\Delta}_{1,a}$, $\underline{\Delta}_{2,a}$, $\overline{\Delta}_{1,a}$ AND $\overline{\Delta}_{2,a}$ UNDER DIFFERENT SHEARING RATES OF SHEARING ATTACKS.

Shear rate	1.0%	2.0%	4.0%	5.0%	6.0%
$\underline{\Delta}_{1,a}$	-0.25	-0.28	-0.32	-0.45	-0.52
$\overline{\Delta}_{1,a}$	0.21	0.32	0.40	0.46	0.58
$\underline{\Delta}_{2,a}$	-0.52	-0.63	-0.74	-1.00	-2.02
$\overline{\Delta}_{2,a}$	0.50	0.63	0.75	1.03	1.32
Stability	$\surd$	$\surd$	$\surd$	$\times$	$\times$

$\surd$ represents the IPS is stable, $\times$ represents the IPS is unstable

To intuitively show performance change of system under different shearing rates of shearing attack, mean and standard deviation (SD) of cart position and pendulum angle are calculated, which are illustrated in Tab. VII of [16]. It can be seen from Tab. VII of [16] that as shearing rate increase, mean and SD of cart position and pendulum angle increase; the greater the shearing rate is, the greater the influence of cart position and pendulum angle is; the performance slightly deteriorates with gradually increasing shearing rates. Tab. VII of [16] also shows that shearing attack has a significant influence on performance of IPS and an efficient image encryption algorithm is required to further improve image security.

V. CONCLUSION

This paper has introduced secure control of NIPVSS with adverse effect of image computation. To meet real-time and security requirements, an F2SIE algorithm was proposed. Adverse effects of image information security were analysed, and the closed-loop model of NIPVSS has been established with computational errors and multiple time-varying delays. Furthermore, a robust controller was designed to tolerate computational errors and multiple time-varying delays, and system stability was examined. Experimental results confirms the effectiveness of the proposed image encryption algorithm and the controller on the NIPVSS platform. In the future, it is a challenge to further reduce image encryption algorithm time, and how to improve performance of encryption algorithm is very interesting and meaningful research venues.

REFERENCES

[1] H. Wu, L. Lou, C.-C. Chen, S. Hirche and K. Kuhnlenz, "Cloud-based networked visual servo control," *IEEE Trans. Ind. Electron.*, vol. 60, no. 2, pp. 554-566, 2013.

[2] D. Cabecinhas, S. Brás, R. Cunha, C. Silvestre and P. Oliveira, "Integrated visual servoing solution to quadrotor stabilization and attitude estimation using a pan and tilt camera," *IEEE Trans. Control Syst. Technol.*, vol. 27, no. 1, pp. 14-29, 2019.

[3] Guang Lu and M. Tomizuka, "Vehicle following as backup control schemes for magnet-magnetometer-based lateral guidance," *IEEE Trans. Control Syst. Technol.*, vol. 13, no. 2, pp. 274-285, 2005.

[4] C.-F. Huang and T.-J. Yeh, "Anti slip balancing control for wheeled inverted pendulum vehicles", *IEEE Trans. Control Syst. Technol.*, vol. 28, no. 3, pp. 1042-1049, 2020.

[5] J. Huang, M. Zhang, S. Ri, C. Xiong, Z. Li and Y. Kang, "High-order disturbance-observer-based sliding mode control for mobile wheeled inverted pendulum systems", *IEEE Trans. Ind. Electron.*, vol. 67, no. 3, pp. 2030-2041, 2020.

[6] W. Ye, Z. Li, C. Yang, J. Sun, C. Su and R. Lu, "Vision-based human tracking control of a wheeled inverted pendulum robot," *IEEE Trans. Cybern.*, vol. 46, no. 11, pp. 2423-2434, 2016.

[7] D. Du, C. Zhang, Y. Song, H. Zhou and W. Li, "Real-time H_∞ control of networked inverted pendulum visual servo systems," *IEEE Trans. Cybern.*, vol. 50, no. 12, pp. 5113-5126, 2020.

[8] D. Ding, Q.-L. Han, X. Ge and J. Wang, "Secure state estimation and control of cyber-physical systems: A survey," *IEEE Trans. Syst. Man Cybern. -Syst.*, vol. 51, no. 1, pp. 176-190, 2021.

[9] J. Zheng and L. Liu, "Novel image encryption by combining dynamic DNA sequence encryption and the improved 2D logistic sine map," *IET Image Process.*, vol. 14, no. 11, pp. 2310-2320, 2020.

[10] C. Chen, K. Sun and Q. Xu, "A color image encryption algorithm based on 2D-CIMM chaotic map," *China Commun.*, vol. 17, no. 5, pp. 12-20, 2020.

[11] K. Hatada, K. Hirata and Y. Masui, "Synthesis of a visual feedback stabilizing controller for an inverted pendulum using a Fisheye lens", in *7th Int. Conf. Control Decis. Inf. Technol.*, pp. 593-598, 2020.

[12] N. Takahashi, O. Sato and M. Kono, "Robust control method for the inverted pendulum system with structured uncertainty caused by measurement error," *Artif. Life Robot.*, vol. 14, no. 4, pp. 574-577, 2009.

[13] Y. Zhang, Q. Zhang, J. Zhang and Y. Wang, "Sliding mode control for fuzzy singular systems with time delay based on vector integral sliding mode surface," *IEEE Trans. Fuzzy Syst.*, vol. 28, no. 4, pp. 768-782, 2020.

[14] S. Yan, M. Shen, S. K. Nguang, G. Zhang and L. Zhang, "A distributed delay method for event-triggered control of T-S fuzzy networked systems with transmission delay," *IEEE Trans. Fuzzy Syst.*, vol. 27, no. 10, pp. 1963-1973, 2019.

[15] X. Li and S. Song, "Stabilization of delay systems: Delay-dependent impulsive control," *IEEE Trans. Autom. Control*, vol. 62, no. 1, pp. 406-411, 2017.

[16] D. Du, C. Zhang, Q. Lu, M. Fei and H. Zhou, "Secure Control of Networked Inverted Pendulum Visual Servo System with Adverse Effects of Image Computation (Extended Version)," 2023, *arXiv:2309.03556*.

[17] L. Kocarev, "Chaos-based cryptography: A brief overview," *IEEE Circuits Syst. Mag.*, vol. 1, no. 3, pp. 6-21, 2001.

[18] R. Li, Q. Liu and L. Liu, "Novel image encryption algorithm based on improved logistic map," *IET Image Process.*, vol. 13, no. 1, pp. 125-134, 2019.

[19] Z. Lin, J. Liu, J. Lian, Y. Ma and X. Zhang, "A novel fast image encryption algorithm for embedded systems," *Multimed. Tools Appl.*, vol. 78, no. 14, pp. 20511-20531, 2019.

[20] W. Li, X. Li, J. Gao and H. Wang, "Design of secure authenticated key management protocol for cloud computing environments," *IEEE Trans. Dependable Secur. Comput.*, vol. 18, no. 3, pp. 1276-1290, 2021.

[21] R.-H. Hsu, J. Lee, T. Q. S. Quek and J.-C. Chen, "GRAAD: Group anonymous and accountable D2D communication in mobile networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 2, pp. 449-464, 2018.

[22] J. Katz and Y. Lindell, *Introduction to modern cryptography*, 2nd ed., ser. Chapman & Hall/CRC Cryptography and Network Security Series. Chapman and Hall/CRC, 2014.

[23] R. Ramasamy and V. Arumugam, "Digital watermarking—A tutorial," *IEEE Potentials*, vol. 41, no. 4, pp. 43-48, 2022.

[24] S. R. Subramanya and B. K. Yi, "Digital signatures," *IEEE Potentials*, vol. 25, no. 2, pp. 5-8, 2006.

[25] D. Du, L. Wu, C. Zhang, Z. Fei, L. Yang, M. Fei, H. Zhou, "Co-design secure control based on image attack detection and data compensation for networked visual control systems," *IEEE Trans. Instrum. Meas.*, vol. 71, pp. 1-14, 2022, Art no. 3524314.

[26] F. Yang, Z. Wang, Y.S. Hung and M. Gani, "H_∞ control for networked systems with random communication delays," *IEEE Trans. Autom. Control*, vol. 51, no. 3, pp. 511-518, 2006.

[27] R. Wang, G.-P. Liu, W. Wang, D. Rees and Y. B. Zhao, "Guaranteed cost control for networked control systems based on an improved predictive control method," *IEEE Trans. Control Syst. Technol.*, vol. 18, no. 5, pp. 1226-1232, 2010.

[28] 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.*, vol. 52, no. 12, pp. 13609-13622, 2022.

[29] Z. Lin, J. Liu, J. Lian, Y Ma and X Zhang, "A novel fast image encryption algorithm for embedded systems," *Multimed. Tools Appl.*, vol. 78, no. 14, pp. 20511-20531, 2019.

[30] S. Winkler and P. Mohandas, "The evolution of video quality measurement: From PSNR to hybrid metrics," *IEEE Trans. Broadcast.*, vol. 54, no. 3, pp. 660-668, 2008.