IEICE TRANSACTIONS

on Information and Systems

DOI:10.1587/transinf.2025MUP0001

Publicized:2025/09/22

This advance publication article will be replaced by the finalized version after proofreading.

A PUBLICATION OF THE INFORMATION AND SYSTEMS SOCIETY

The Institute of Electronics, Information and Communication Engineers

Kikai-Shinko-Kaikan Bldg., 5-8, Shibakoen 3 chome, Minato-ku, TOKYO, 105-0011 JAPAN

PAPER

Cyber-Physical Steganography in Robotic Motion Control

Ching-Chun CHANG[†a)], **Yijie LIN**[††], ***Nonmembers***, ***and*** **Isao ECHIZEN**[†††], ***Fellow***

SUMMARY Steganography, the art of information hiding, has continually evolved across visual, auditory and linguistic domains, adapting to the ceaseless interplay between steganographic concealment and steganalytic revelation. This study seeks to extend the horizons of what constitutes a viable steganographic medium by introducing a steganographic paradigm in robotic motion control. Based on the observation of the robot's inherent sensitivity to changes in its environment, we propose a methodology to encode messages as environmental stimuli influencing the motions of the robotic agent and to decode messages from the resulting motion trajectory. The constraints of maximal robot integrity and minimal motion deviation are established as fundamental principles underlying secrecy. As a proof of concept, we conduct experiments in simulated environments across various manipulation tasks, incorporating robotic embodiments equipped with generalist multimodal policies.

key words: *artificial intelligence, cyberphysics, robotics, steganography*

1. Introduction

Steganography, the art of concealing information within non-suspicious media, is rooted in the exchange of messages, which has always carried with it the timeless challenge of secrecy [1–6]. From whispers in shadows to the hidden messages written in the margins of history, humankind has long sought ways to convey thoughts that remain imperceptible to all but the chosen few. This ancient pursuit of covert communication has evolved, stretching across the realms of visual, auditory, and linguistic media [7–13]. In the intricate patterns of imagery, the subtle modulation of sound and the carefully crafted structures of language, steganography advances in various forms, continually adapting to the evolving steganalytic detection mechanisms that seeks to reveal hidden messages [14–20].

This study embarks on an exploration of a new steganographic paradigm in robotics, the realm where the cyber and physical worlds intersect, expanding the boundaries of what is considered a viable channel for covert communication. We consider a form of steganography through the very motions of a robotic agent. Robotics is an interdisciplinary study dedicated to the pursuit of intelligent behaviours that mimic human actions [21]. At the heart of this quest lies robotic motion control, a domain that spans automation from basic manipulation to complex interaction with dynamic environments [22]. The integration of artificial intelligence, particularly reinforcement learning, has endowed robotic agents with a high level of autonomy, enabling them to learn, adapt and optimise their decision-making policies over time [23–25].

It is conceivable to design learning algorithms that adjust a robot's policies for the purpose of steganography, guiding it to embed hidden messages within its very motions. However, a legitimate robot may have integrity regulations in place to protect the fundamental ethical and safety guidelines programmed into its underlying control model [26–28]. Any unauthorised attempts to modify the robot might not go unnoticed. Such illicit manipulations could trigger alarms and activate built-in safeguard mechanisms to prevent catastrophic consequences. Thus, we propose a research challenge, one that requires steganographic methodology in robotics to adhere to the constraint of perfect robot integrity.

In this study, we introduce a steganographic methodology in the context of robotic motion control, subject to the constraint of perfect robot integrity. We exploit the robot's sensitivity to environmental fluctuations, representing messages as subtle deviations in its motion trajectory. The causal relationships between the influencing factors and the message symbols are established through a trial-and-error heuristic in a simulated virtual environment, until each message symbol is uniquely represented. The synchronised encoding and decoding processes are then applied in the physical world, where the robot's motion trajectory serves as the medium for transmitting secret information.

The remainder of this paper is organised as follows. Section 2 outlines the key concepts in robotic motion control that underpin this study. Section 3 formalises the problem and methodology for steganography in robotic motion control. Section 4 explores the statistical aspects of capacity settings through theoretical analysis. Section 5 presents the experimental validation across various motion control tasks and multimodal robotic agents, including visualisations of simulated environments and performance evaluations on secrecy and capacity. Finally, Section 6 concludes the paper with a summary of research findings and potential future directions.

2. Foundations of Robotics

This section provides a brief introduction to fundamental concepts and terminology in robotic motion control, which are relevant to the development of the steganographic methodology.

[†]National Institute of Informatics, Japan
[††]Feng Chia University, Taiwan
[†††]University of Tokyo, Japan
a) E-mail: ccchang@nii.ac.jp

2.1 Dynamical Simulation

The field of robotics has been propelled by the quest for developing *generalist robotic policies* capable of handling a broad spectrum of tasks, including manipulation, grasping and assembly, with precision and autonomy [29]. To evaluate robotic policies, *real-world benchmarks* are crucial as they provide assessments in uncontrolled environments, with varying environmental factors such as lighting conditions, material properties and sensor errors [30]. However, real-world evaluation is hindered by several limitations, including resource-demanding and time-consuming setup and maintenance. Additionally, it faces challenges in scalability and reproducibility, as testing a wide variety of conditions efficiently and ensuring consistent experimental conditions in dynamic real-world environments can be difficult.

These constraints become particularly evident as robotic systems are deployed in complex environments, driving a shift toward *simulation-based evaluations* as a more cost-efficient, scalable and reproducible alternative. Simulators equipped with *physics engines* offer a sufficiently realistic approximation of physical systems, capturing the essential dynamics that allow robots to be evaluated under controlled virtual conditions [31–34]. These simulations can mimic the dynamics of real-world interactions, enabling the evaluation of robotic policies across various scenarios with unlimited trails. The flexibility to subtly manipulate various environmental factors, coupled with the capability for repeated trials, provides an ideal platform for the proposed steganographic methodology.

2.2 Mechanical Robot

A robot is a physical agent equipped with sensors, actuators and computational resources. It interacts with the environment by perceiving states through its sensors and taking actions autonomously via its actuators [35]. A robot's actions are governed by an underlying policy model, which maps the sensed state to an optimal action [36]. In reinforcement learning, this policy is often learned through interactions with the environment to maximise cumulative rewards [37–41]. The development of multimodal robotic agents has advanced robotic motion control through the integration of multiple sensory modalities such as auditory, visual and linguistic information [42–45]. These multimodal sensors enhance contextual awareness and human-machine interaction, enabling robots to respond more intelligently and interact more naturally with human operators. For example, a visual-language-action robotic agent can process visual scenes to understand the context of the environment and interpret linguistic commands from humans to execute specific actions

A robotic arm is an articulated mechanical manipulator designed to replicate the functions of a human arm, serving as an ideal example for demonstrating robotic motion control [46]. It positions and orients an end effector in three-dimensional space, much as a human arm directs the hand. Robotic arms are widely used in industrial applications due to their versatility in executing complex manoeuvres. A kinematic chain with 6 or 7 degrees of freedom (DOF) typically comprises a shoulder (two or three rotary joints), an elbow (one rotary joint), a wrist stack (three rotary joints), and a hand (a separate functional axis). An actuated arm (with over 6 DOF) exhibits motions that can be generally categorised into the following primary types:

- Positional motion that moves the position of the end effector in a linear direction along predefined axes (X, Y and Z).
- Rotational motion that adjusts the orientation of the end effector (pitch, yaw and roll).
- Functional motion that controls the gripping mechanism of the end effector such as claws or fingers to grasp or release.

This study aims to develop a steganographic methodology capable of seamlessly operating within scenarios involving modern robotic agents.

3. Steganography in Robotics

This section outlines the methodology for steganography in the context of robotic motion control. We begin by presenting the problem formulation, which defines the core components and constraints of the research. Following that, a trial-and-error heuristic is introduced, leveraging the robot's sensitivity to environmental changes for covert communication of secret information

3.1 Problem Formulation

We present a formal problem of steganography applied to robotics, where the objective is to covertly encode a secret message into the motions of a robot. The sender Alice influences the robot's motions while it is tasked with performing a predefined mission. The receiver Bob observes the motion signal from a remote location and decodes the secret message embedded in the motions. This subliminal communication should not significantly interfere with the robot's normal operations for the secrecy requirement.

Formally, let the robot's motion trajectory be defined as a sequence of actions $\mathbf{a} = \{a_1, a_2, \ldots, a_T\}$, where each action $a_t \in \mathbb{R}^n$ at time step t specifies the desired state of the end-effector, including its positional, orientational, and functional motions. The total number of time steps is denoted by T. The action space represents high-level motion intents in end-effector-level control. To execute these actions, inverse kinematics is used to infer the underlying joint configurations required to realise each end-effector state. The robot's decision process is governed by a pre-trained control model, which determines how the robot acts and moves from an initial state to a terminal state. Specifically, we consider a vision-language-action model that integrates visual perception and language understanding to guide the robot's actions

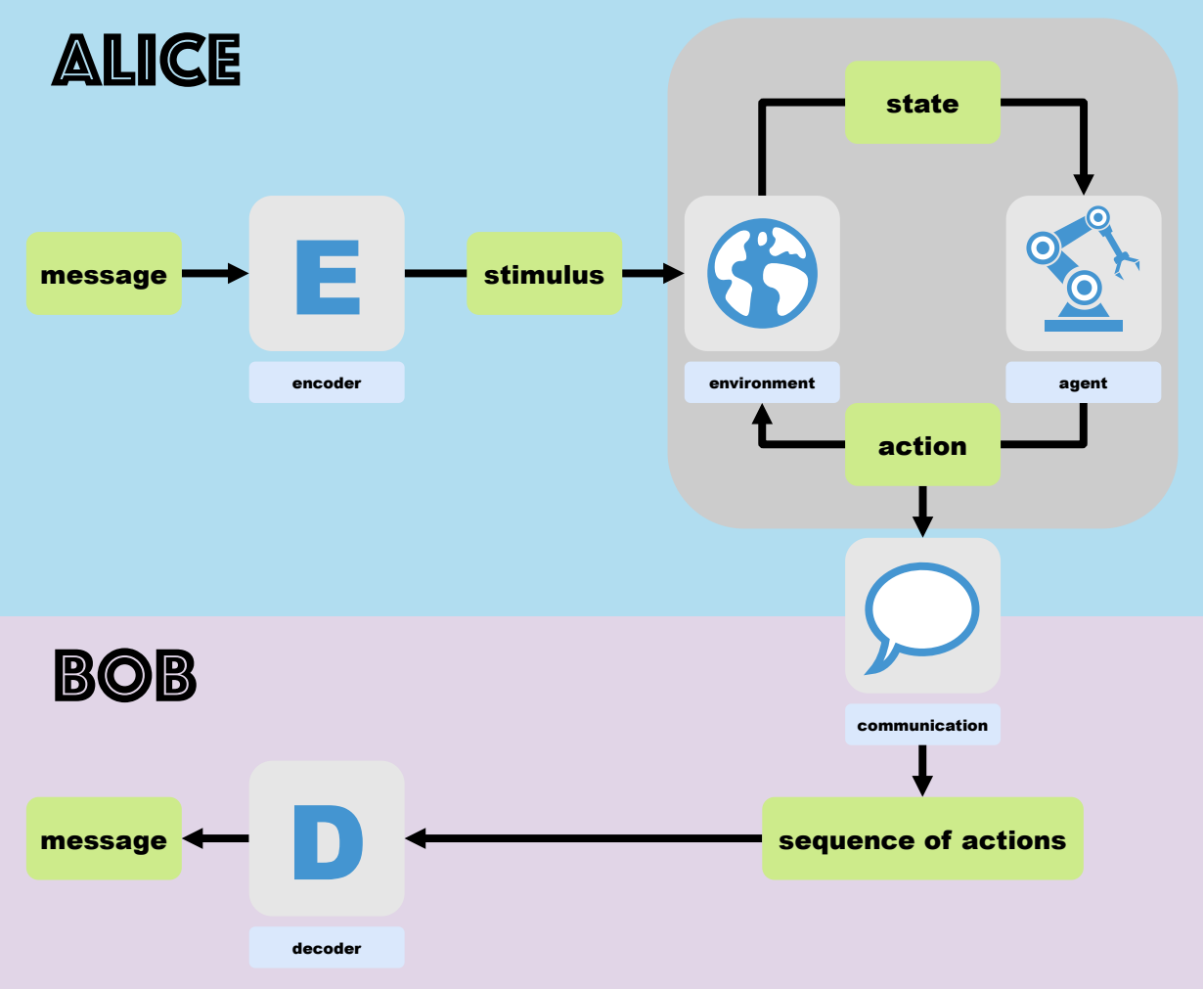


Fig. 1: Overview of steganography in robotic motion control: Alice encodes a message as a stimulus that affects the interaction between the robotic agent and the environment, whereas Bob decodes the message from the sequence of actions transmitted via the robot's in-built communication system.

through multimodal reasoning.

Alice, who is located in the same environment as the robot, can stimulate subtle deviations in the motion trajectory to encode an intended secret message m. Bob, located remotely, can observe the motion trajectory $\mathbf{a}$ from which the message m is decoded. The motion signal is transmitted as part of the robot's built-in communication system, which is designed for real-time monitoring and tracking of the robot's operations to support diagnostics and ensure safety. Some sensitive data, such as camera scenes, may be unavailable for analysis due to privacy regulations. In this context, Alice exploits the robot's surveillance system to communicate secretly with Bob, who disguises himself as an authorised observer and gains access to the motion signal under the pretence of performing legitimate maintenance duties. In this steganographic framework, the following core constraints are applied.

- Maximal Robot Integrity: The robot's underlying control model is protected from unauthorised tampering or retraining, which could lead to malfunction or unintended behaviours, thereby jeopardising the safety of the environment in which the robot operates. Any attempt to modify the predefined model parameters may be detected, triggering alarms or other built-in safeguard mechanisms.
- Minimal Motion Deviation: The robot's motion trajectory is required to align with the expected motion statistics. An excessive deviation from the typical trajectory may signal a malfunction or raise steganalytic suspicions, triggering an automatic halt in operation for further investigation.

Note that while cyber-physical gaps and observational errors, which may arise due to simulation imperfection, actuation precision, communication noise or sensor limitation, are not always negligible, the scope of this study is focused on a prototypical setting to establish foundational principles.

3.2 Trail-and-Error Heuristic

The robot's control model can be sensitive to *environmental stimuli*, meaning that changes in the surroundings, such as the introduction of new objects or variations in the background, can affect its decision-making processes. These changes may lead to deviations in the robot's planned trajectory or force it to adapt its actions to accommodate and account for the new environmental factors. On the one hand, such sensitivity could potentially enhance the robot's ability to operate in dynamic environments; on the other hand, it also exposes potential vulnerabilities, as unforeseen environmental changes can cause unintended consequences that disrupt the robot's normal functioning.

In view of this, we propose a trial-and-error heuristic that exploits the robot's sensitivity to environmental changes for encoding and decoding hidden messages, as illustrated in Figure 1. Initially, Alice and Bob agree upon a common *stego-key*, which serves as the seed for initialising a shared decoder, ensuring the synchronisation of encoding and decoding processes. According to Kerckhoffs's principle and Shannon's maxim in cryptography, one ought to assume that the enemy knows the system [47]. A system should be secure, even if everything about the system, except the key, is public knowledge. In other words, the security of a system should not rely on the secrecy of the algorithm, but rather on the secrecy of the key. In a steganographic system, the security is governed by a stego-key, which coordinates the operations between the two parties, Alice and Bob.

Alice exploits the robot's sensitivity to environmental changes by sampling and placing subtle stimuli in its environment, which influence the robot's motion trajectory. Each resulting motion trajectory can be mapped to a message symbol by the shared decoder, which, being a many-to-one function, may produce duplicate symbols. Therefore, the process is iterated (in a simulated cyber environment), following a trial-and-error heuristic, with stimuli being resampled until all unique message symbols are represented. Once the set of stimuli corresponding to the entire symbol space has been established, these stimuli are applied (in the physical world) to encode any secret message, which is then communicated in the form of a motion trajectory. Bob, located remotely, observes the motion trajectory and uses the shared decoder to extract the hidden message. This method preserves the integrity of the robot's control model while allowing for asymptotically minimal deviation as the number of trials increases. A step-by-step methodology is outlined as follows.

• Initialisation of Decoder: Alice and Bob exchange a common stego-key, from which the shared decoder is initialised, as denoted by

$$\mathcal{D} = \text{init}(k). \tag{1}$$

Table 1: Comparison of empirical, theoretical and approximate means.

n	**Empirical Mean**	**Theoretical Mean**	**Approximate Mean**
2	02.99	03.00	02.54
3	05.51	05.50	05.03
4	08.37	08.33	07.85
5	11.32	11.42	10.93
6	14.57	14.70	14.21
7	18.22	18.15	17.66
8	21.67	21.74	21.25

This decoder function serves as a mapping from the action sequence to the message space $\mathcal{M}$.

• Initialisation of Encoder: Alice randomly samples a stimulus ψ and places it within the simulated cyber environment, causing a slight environmental change. The sequence of actions is generated though the interactions between the robot and its environment in the presence of the stimulus ψ, as given by

$$\mathbf{a} = \text{interact}(\psi). \tag{2}$$

This action sequence is then mapped to a message symbol by the shared decoder. The process is iterative, with new stimuli being resampled and trials executed until the set of decoded symbols covers all possible symbols in the message space $\mathcal{M}$. Therefore, each distinct message symbol can be encoded as an environmental stimulus, as represented by

$$\psi_m = \mathcal{E}(m). \tag{3}$$

For symbols that correspond to more than one stimulus, the stimulus resulting in the optimal motion trajectory (which minimises time costs or maximises efficiency) can be chosen.

• Encoding process: On the transmitting side, Alice encodes the intended message as its corresponding stimulus and positions it in the physical environment, influencing the robot's motion during its interactions with the environment, as expressed by

$$\mathbf{a} = \text{interact}(\mathcal{E}(m)). \tag{4}$$

• Decoding process: At the receiving end, Bob applies the shared decoder to the observed motion trajectory and extracts the hidden message by

$$m = \mathcal{D}(\mathbf{a}). \tag{5}$$

4. Theoretical Analysis

The code construction begins by fixing the decoder, and then establishes the encoder by randomly sampling codes (stimuli) until every symbol in the message space is uniquely represented by at least one sampled code. The capacity is

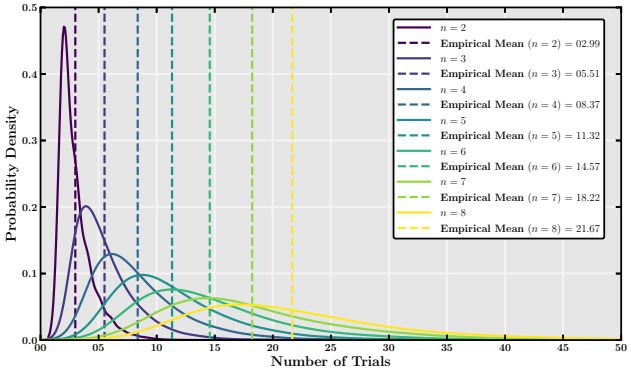


Fig. 2: Expected number of trials required for complete coverage of message space.

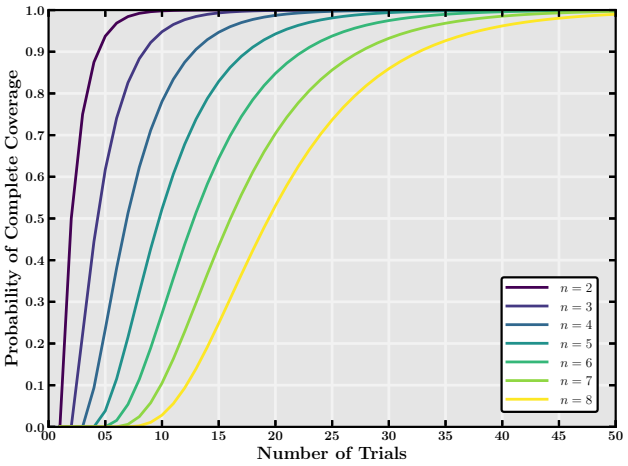


Fig. 3: Probability of complete coverage with respect to the number of trials conducted.

calculated as the binary logarithm of the message space size, $\log_2 \|\mathcal{M}\|$, with the unit expressed in bits per trajectory. The main challenge in this process lies in determining how many random codes must be sampled to achieve complete coverage of all message symbols with high confidence. This section seeks to answer questions of how many trials are needed to ensure success with high confidence and how likely is complete coverage after a given number of trials.

4.1 Random Coding

The trial-and-error heuristic can be implemented using a decoder constructed with hashing and modular arithmetic. Specifically, the decoder employs a keyed hash function followed by modular reduction to ensure that all possible codes are confined to the fixed range of the message space, as expressed by

$$m = \text{hash}(\psi_m) \mod \|\mathcal{M}\| \tag{6}$$

This decoder deterministically maps each sampled code to a symbol within the message space. The uniformity of the hash function minimises the likelihood of uneven distribution, ensuring that symbols in the message space are approximately equally represented. This uniformity allows for straightforward theoretical analysis of the relationships between the number of trials and the full coverage the message space. Note that, despite its theoretical simplicity, this decoding approach is sensitive to errors which might arise in practical implementations. Although addressing the robustness limitations lies beyond the scope of this study, further investigation into a more adaptable decoding mechanism could enhance resilience against errors.

4.2 Expected Number of Trials

The problem of determining the required number of random codes to cover all n message symbols is analogous to the *coupon collector's problem* in probability theory. This problem concerns the expected time (number of trials) to collect all n distinct items (coupons), assuming each trial independently and uniformly selects one item. This expected value is given by

$$\mathbb{E}[T_n] = n \cdot \left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}\right) = n \cdot H_n, \tag{7}$$

where where H_n is the n-th harmonic number (the sum of the reciprocals of the first n natural numbers). The n-th harmonic number is about as large as the natural logarithm of n by approximating the sum with the integral:

$$H_n = \sum_{k=1}^{n} \frac{1}{k} \approx \int_1^n \frac{1}{x} dx = \ln n, \tag{8}$$

As n goes to infinity, the difference between the harmonic series and the natural logarithm approaches asymptotically towards the limit known as the Euler-Mascheroni constant:

$$\lim_{n\to\infty} (H_n - \ln n) = \gamma. \tag{9}$$

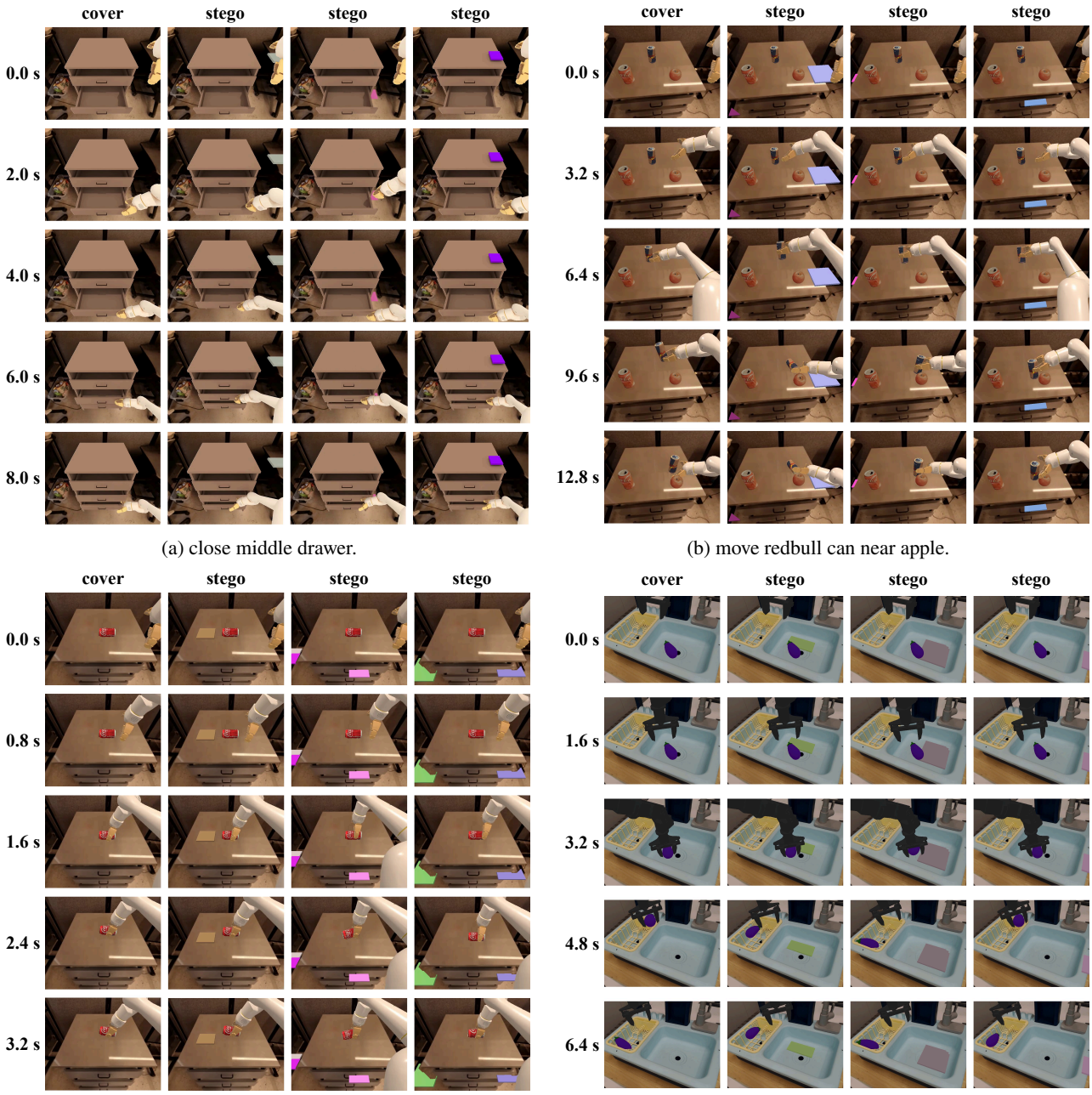
Given the asymptotic behaviour of the harmonic number, the expected value can be approximated as

$$n \cdot H_n \sim n \cdot (\ln n + \gamma)\,. \tag{10}$$

This results characterises the expected behaviour of the sampling process and highlights that collecting the final few items takes disproportionately longer than the initial ones, a phenomenon often referred to as the *diminishing returns*. Table 1 compares the mean values across different message space sizes, obtained from empirical simulation, theoretical derivation and asymptotic approximation. Figure 2 illustrates the empirical mean of the required trials computed over 10,000 simulations, with the distribution approximated using kernel density estimation on the empirical data.

4.3 Probability of Complete Coverage

Another central question concerns the probability of complete coverage after t trials. Instead of directly calculating



(a) close middle drawer.

(b) move redbull can near apple.

(c) pick coke can.

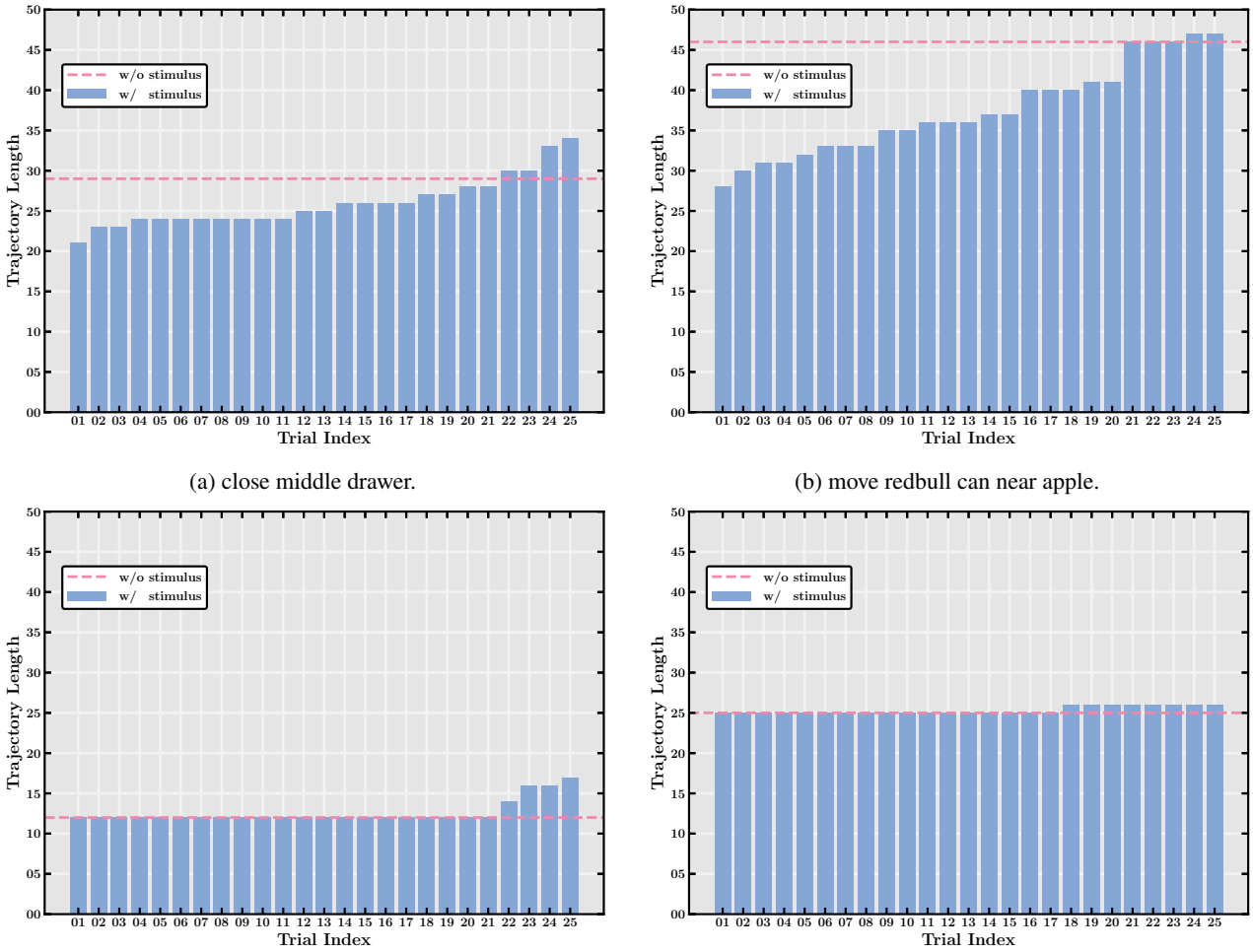
(d) put aubergine into yellow basket.

Fig. 4: Visualisation of robotic motion control: each column represents a motion trajectory with the non-stimulated one (cover) shown in the first column and steganographic variations (stego) in the rest, whereas each row shows successive time snapshots with equally spaced intervals for each task (in seconds).

the probability that all n items are drawn, we begin by finding the probability that at least one item is not drawn after t trials and then subtract this from 1. For at least one item to remain uncollected, there must exist a subset of k items (where $1 \leq k \leq n$) that are not collected at all. The probability that exactly k specific items are not drawn after t trials is given by

$$\binom{n}{k}\left(\frac{n-k}{n}\right)^t. \tag{11}$$

When calculating the probability that at least one item is not drawn, overlaps between subsets of uncollected items must be carefully accounted for. The *inclusion-exclusion principle* addresses this by alternately adding and subtracting probabilities of subsets of increasing size. Starting with the probability of missing single items, we subtract probabili-



(a) close middle drawer.

(b) move redbull can near apple.

(c) pick coke can.

(d) put aubergine into yellow basket.

Fig. 5: Secrecy analysis based on the statistics of trajectory lengths.

ties for pairs of missing items to correct overcounting, then add probabilities for triples to correct undercounting, and so on. This alternating process handles all overlaps, leading to the probability that at least one item is not drawn after t trials. Finally, subtracting this from 1 gives the likelihood of achieving complete coverage in a finite number of trials:

$$\mathbb{P}(t) = 1 - \sum_{k=1}^{n} (-1)^{k+1} \binom{n}{k} \left(\frac{n-k}{n}\right)^{t}. \tag{12}$$

Figure 3 illustrates the probability of achieving complete coverage as a function of the number of trials, demonstrating how a larger number of items requires more trials to reach a comparable probability.

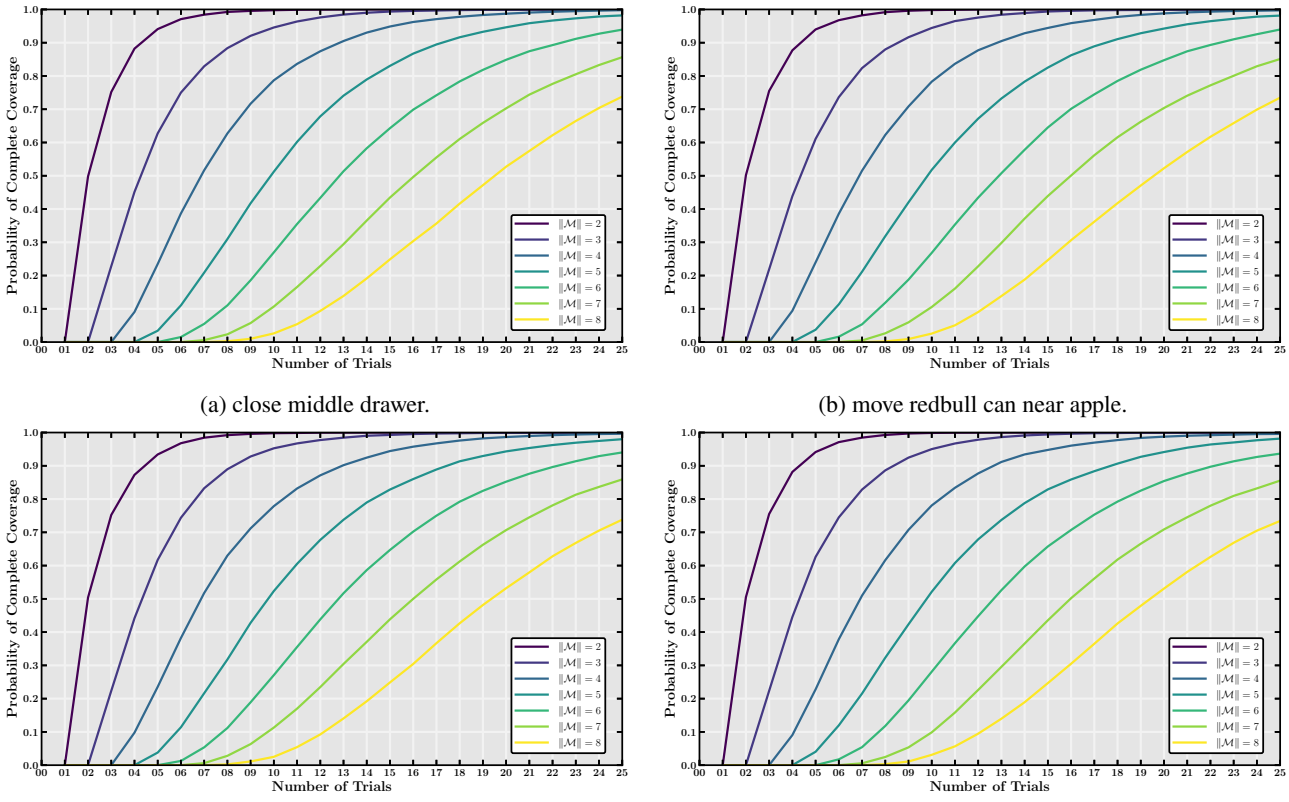
5. Experiments

This section presents experimental evaluations. It begins with a description of the simulation setup, followed by a visualisation of motion trajectories through a simulation interface. The steganographic performance is assessed in terms of both secrecy and capacity.

5.1 Simulation Setup

Our evaluations spanned four distinct tasks in a dynamical simulator [48]: closing the middle drawer, moving a Red Bull can near an apple, picking up a Coke can, and placing an aubergine into a yellow basket. These tasks were performed by two robotic embodiments: the first three tasks were executed by the Google robotic arm, while the last task was carried out by the WidowX robotic arm. The robotic embodiments were controlled by two multimodal policy models: the motions in the first two tasks were governed by OpenVLA [49], while the motions in the latter two tasks were directed by Octo [50].

Despite the differences in kinematics and control, our steganographic procedure remains unaffected, because it operates exclusively at the motion level and is thus agnostic to any particular joint layout. Naturally, each robotic embodiment exhibits its own physical adaptability to certain movements and objects, and each control model inherits limitations from the data available during training. Con-



(a) close middle drawer.

(b) move redbull can near apple.

(c) pick coke can.

(d) put aubergine into yellow basket.

Fig. 6: Capacity analysis based on the probability of complete coverage over the message space.

sequently, every arm-policy pair has inherent strengths and weaknesses that become more or less pronounced across different tasks and environmental conditions. Our experimental setup was chosen empirically: for each task we selected the robotic embodiment and controller that were well-suited to deliver reliable execution.

For each task, there were 25 steganographic trajectories generated through trials of sampling random objects as environmental stimuli, alongside one original trajectory serving as a referential baseline. To obtain statistically reliable results, the experiments were conducted with 10,000 pseudo-randomly generated keys, each used to initialise a unique decoder.

5.2 Visualisation

Figure 4 visualises the motion trajectories executed by a robotic agent for each task in both conditions, with and without stimuli. This visualisation highlights how environmental stimuli subtly influence the motion trajectories, with minimal observable deviations between the baseline and steganographic trajectories. These environmental stimuli were instantiated as monochromatic shape objects placed in random locations to simplify the demonstration of the methodology. In practice, stimuli can be arbitrarily and flexibly designed as any objects to suit the contextual secrecy requirements of specific environments. The motion deviations arise because the stimuli alter the visual scene perceived by the vision–language–action planner, prompting it to produce slightly perturbed yet still task-compliant actions. The resultant action sequence nevertheless leads to the same goal state, a behaviour analogous to trajectories in chaotic dynamical systems converging on an attractor.

5.3 Secrecy Analysis

We evaluated secrecy via the statistics of trajectory lengths. Figure 5 depicts the lengths of steganographic trajectories compared to the length of the non-stimulated trajectory. The deviations in trajectory lengths reflect the steganographic impact, which did not result in a monotonic increase or decrease the task completion times. Instead, unpredictable variations were observed in the lengths of steganographic trajectories. While these deviations in trajectory lengths provide an initial indication of the potential inconspicuousness of the steganographic system, this metric alone may not fully capture the comprehensive statistics related to secrecy. To the best of our knowledge, no steganalysis methods have been specifically developed for steganography in robotic motion control at the time of writing, making this an emerging area for further exploration.

5.4 Capacity Analysis

We evaluated capacity with respect to the probability of complete coverage over the message space. Figure 6 demonstrates this probability as a function of the number of trials, evaluated across 10,000 randomly initialised decoders. The simulations were conducted for various message space sizes, ranging from 2 to 8 symbols, corresponding to capacity settings of 1 to 3 bits (calculated as binary logarithm of the message space size). The curves highlight the progressive increase in the probability of success with an increasing number of trials. The results underscore the balance between capacity and efficiency, demonstrating that smaller message spaces enable faster convergence, whereas larger spaces necessitate additional trials to maintain high coverage probabilities.

6. Conclusions

This study introduced a steganographic paradigm in robotic motion control, exploring the robot's sensitivity to environmental stimuli to allow covert communication via motion trajectories. Following the formulated principles regarding maximal robot integrity and minimal motion deviation, we demonstrated how a message can be encoded as an environmental stimulus that influences the interactions between the robotic agent and the environment and how this message can be decoded from the resulting motion trajectory.

In contrast to conventional carrier signals such as images, audio and text, robotic motion offers distinctive advantages yet poses new challenges for steganography. On the one hand, an adversary seldom possesses perfectly time-synchronised motion data: recording trajectories at the required temporal resolution demands specialised hardware, whereas bit-perfect copies of digital files are readily obtained and inspected. Moreover, steganalysis tools for robotic motion remain nascent at the time of writing, affording it a temporary security advantage over digital media, which have been subjected to decades of well-documented attacks. On the other hand, the physical nature of robotic motion imposes stringent reliability constraints, thereby limiting payload capacity and necessitating careful trade-offs between secrecy, robustness and fidelity in task performance.

This study initiates a broader enquiry, with potential limitations to address and future directions to pursue:

- First, an exploitation of higher-order kinematic descriptors such as velocity and acceleration may serve as secrecy metrics that complement simple path length by capturing how quickly and smoothly the robot progresses from start to goal. Even if a covert stimulus leaves the overall path length unchanged, it can introduce subtle deviations in kinematic profiles. Such dynamic nuances can therefore be used to flag atypical stego trajectories whose kinematic profiles deviate from task norms.
- Second, a rigorous secrecy evaluation via steganalysis is necessary to assess vulnerability to analytical detection mechanisms tailored to robotic motion. Potential steganalytic methods include distributional-divergence tests, such as relative entropy, and temporal-similarity measures, such as dynamic time warping, applied to cover and stego action trajectories. Complementing these statistical tools, machine learning classifiers can be trained to identify higher-level abnormalities that lie beyond the reach of classical analyses.
- Third, real-world contingencies such as cyber-physical gaps, environmental noise, sensor drift, observational imperfections, intermittent occlusion and the presence of an active adversary could compromise the reliability of steganographic communication. Such disturbances may distort the observed trajectories and desynchronise the encoder–decoder pair, thereby posing a risk of false message extraction. Robustness against such errors at the receiving end warrants investigation.

We envision that the concept of cyber-physical steganography in robotics will pave the way for broadening the scope of what constitutes viable channels for steganography.

Acknowledgements

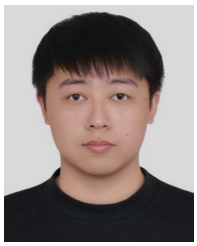
This work was supported in part by the Japan Society for the Promotion of Science (JSPS) under KAKENHI Grants (JP21H04907 and JP24H00732), and in part by the Japan Science and Technology Agency (JST) under CREST Grant (JPMJCR20D3) including AIP Challenge Program, AIP Acceleration Grant (JPMJCR24U3) and K Program Grant (JPMJKP24C2).

References

[1] D. Kahn, "The history of steganography," in *Proc. Int. Workshop Inf. Hiding (IH)*, Cambridge, UK, 1996, pp. 1–5.
[2] N. F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen," *Computer*, vol. 31, no. 2, pp. 26–34, 1998.
[3] R. Anderson and F. Petitcolas, "On the limits of steganography," *IEEE J. Sel. Areas Commun.*, vol. 16, no. 4, pp. 474–481, 1998.
[4] F. Petitcolas, R. Anderson, and M. Kuhn, "Information hiding—a survey," *Proc. IEEE*, vol. 87, no. 7, pp. 1062–1078, 1999.
[5] D. Artz, "Digital steganography: Hiding data within data," *IEEE Internet Comput.*, vol. 5, no. 3, pp. 75–80, 2001.
[6] J. Fridrich, *Steganography in Digital Media: Principles, Algorithms, and Applications*. Cambridge, UK: Cambridge University Press, 2009.
[7] P. Wayner, "Mimic functions," *Cryptologia*, vol. 16, no. 3, pp. 193–214, 1992.
[8] D. Gruhl, A. Lu, and W. Bender, "Echo hiding," in *Proc. Int. Workshop Inf. Hiding (IH)*, Cambridge, UK, 1996, pp. 295–315.
[9] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," *IBM Syst. J.*, vol. 35, no. 3&4, pp. 313–336, 1996.
[10] J. Fridrich, M. Goljan, P. Lisonek, and D. Soukal, "Writing on wet paper," *IEEE Trans. Signal Process.*, vol. 53, no. 10, pp. 3923–3935, 2005.
[11] C.-Y. Chang and S. Clark, "Practical linguistic steganography using contextual synonym substitution and a novel vertex coding method," *Comput. Linguist.*, vol. 40, no. 2, pp. 403–448, 2014.

[12] J. Zhu, R. Kaplan, J. Johnson, and L. Fei-Fei, "HiDDeN: Hiding data with deep networks," in *Proc. Eur. Conf. Comput. Vis. (ECCV)*, Munich, Germany, 2018, pp. 682–697.
[13] Z. Ziegler, Y. Deng, and A. Rush, "Neural linguistic steganography," in *Proc. Conf. Empir. Methods Nat. Lang. Process. (EMNLP)*, Hong Kong, China, 2019, pp. 1210–1215.
[14] A. Westfeld and A. Pfitzmann, "Attacks on steganographic systems," in *Proc. Int. Workshop Inf. Hiding (IH)*, Dresden, Germany, 2000, pp. 61–76.
[15] H. Farid, "Detecting hidden messages using higher-order statistical models," in *Proc. Int. Conf. Image Process.*, vol. 2, Rochester, NY, USA, 2002, pp. 905–908.
[16] N. Provos and P. Honeyman, "Hide and seek: An introduction to steganography," *IEEE Secur. Priv.*, vol. 1, no. 3, pp. 32–44, 2003.
[17] A. D. Ker, T. Pevný, J. Kodovský, and J. Fridrich, "The square root law of steganographic capacity," in *Proc. ACM Workshop Multimed. Secur.*, Oxford, UK, 2008, pp. 107–116.
[18] J. Kodovský, J. Fridrich, and V. Holub, "Ensemble classifiers for steganalysis of digital media," *IEEE Trans. Inf. Forensics Secur.*, vol. 7, no. 2, pp. 432–444, 2012.
[19] J. Fridrich and J. Kodovský, "Rich models for steganalysis of digital images," *IEEE Trans. Inf. Forensics Secur.*, vol. 7, no. 3, pp. 868–882, 2012.
[20] G. Xu, H. Wu, and Y.-Q. Shi, "Structural design of convolutional neural networks for steganalysis," *IEEE Signal Process. Lett.*, vol. 23, no. 5, pp. 708–712, 2016.
[21] T. Yoshikawa, *Foundations of robotics*. Cambridge, MA, USA: MIT Press, 1990.
[22] B. Donald, P. Xavier, J. Canny, and J. Reif, "Kinodynamic motion planning," *J. ACM*, vol. 40, no. 5, pp. 1048–1066, 1993.
[23] R. Sutton and A. Barto, *Reinforcement Learning: An Introduction*. Cambridge, MA, USA: MIT Press, 1998.
[24] V. Mnih *et al.*, "Human-level control through deep reinforcement learning," *Nature*, vol. 518, no. 7540, pp. 529–533, 2015.
[25] K. M. Collins *et al.*, "Building machines that learn and think with people," *Nat. Hum. Behav.*, vol. 8, no. 10, pp. 1851–1863, 2024.
[26] L. Floridi *et al.*, "AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations," *Minds Mach.*, vol. 28, no. 4, pp. 689–707, 2018.
[27] J. Whittlestone, R. Nyrup, A. Alexandrova, and S. Cave, "The role and limits of principles in AI ethics: Towards a focus on tensions," in *Proc. AAAI/ACM Conf. AI Ethics Soc. (AIES)*, Honolulu HI USA, 2019, pp. 195–200.
[28] A. F. Winfield, K. Michael, J. Pitt, and V. Evers, "Machine ethics: The design and governance of ethical AI and autonomous systems [scanning the issue]," *Proc. IEEE*, vol. 107, no. 3, pp. 509–517, 2019.
[29] R. M. Murray, S. S. Sastry, and L. Zexiang, *A Mathematical Introduction to Robotic Manipulation*. Boca Raton, FL, USA: CRC Press, 1994.
[30] N. Correll *et al.*, "Analysis and observations from the first Amazon picking challenge," *IEEE Trans. Autom. Sci. Eng.*, vol. 15, no. 1, pp. 172–188, 2018.
[31] N. Koenig and A. Howard, "Design and use paradigms for Gazebo, an open-source multi-robot simulator," in *Proc. IEEE/RSJ Int. Conf. Intell. Robot. Syst. (IROS)*, vol. 3, Sendai, Japan, 2004, pp. 2149–2154.
[32] E. Todorov, T. Erez, and Y. Tassa, "MuJoCo: A physics engine for model-based control," in *Proc. IEEE/RSJ Int. Conf. Intell. Robot. Syst. (IROS)*, Vilamoura-Algarve, Portugal, 2012, pp. 5026–5033.
[33] E. Rohmer, S. P. N. Singh, and M. Freese, "V-REP: A versatile and scalable robot simulation framework," in *Proc. IEEE/RSJ Int. Conf. Intell. Robot. Syst. (IROS)*, Tokyo, Japan, 2013, pp. 1321–1326.
[34] V. Makoviychuk *et al.*, "Isaac Gym: High performance GPU based physics simulation for robot learning," in *Proc. Int. Conf. Neural Inf. Process. Syst. (NeurIPS)*, Virtual Event, 2021, pp. 1–12.
[35] A. Ijspeert, J. Nakanishi, and S. Schaal, "Movement imitation with nonlinear dynamical systems in humanoid robots," in *Proc. IEEE Int. Conf. Robot. Autom. (ICRA)*, vol. 2, Washington, DC, USA, 2002, pp. 1398–1403.
[36] R. Bellman, "A markovian decision process," *J. Math. Mech.*, vol. 6, no. 5, pp. 679–684, 1957.
[37] R. S. Sutton, "Learning to predict by the methods of temporal differences," *Mach. Learn.*, vol. 3, no. 1, pp. 9–44, 1988.
[38] C. J. C. H. Watkins, "Learning from delayed rewards," Ph.D. dissertation, King's College, University of Cambridge, Cambridge, UK, 1989.
[39] L.-J. Lin, "Self-improving reactive agents based on reinforcement learning, planning and teaching," *Mach. Learn.*, vol. 8, no. 3, pp. 293–321, 1992.
[40] R. J. Williams, "Simple statistical gradient-following algorithms for connectionist reinforcement learning," *Mach. Learn.*, vol. 8, no. 3, pp. 229–256, 1992.
[41] R. S. Sutton, D. McAllester, S. Singh, and Y. Mansour, "Policy gradient methods for reinforcement learning with function approximation," in *Proc. Int. Conf. Neural Inf. Process. Syst. (NeurIPS)*, vol. 12, Denver, CO, USA, 1999, pp. 1057–1063.
[42] J. Ngiam, A. Khosla, M. Kim, J. Nam, H. Lee, and A. Y. Ng, "Multimodal deep learning," in *Proc. Int. Conf. Mach. Learn. (ICML)*, Bellevue, WA, USA, 2011, pp. 689–696.
[43] N. Srivastava and R. Salakhutdinov, "Multimodal learning with deep Boltzmann machines," *J. Mach. Learn. Res.*, vol. 15, no. 84, pp. 2949–2980, 2014.
[44] T. Baltrušaitis, C. Ahuja, and L.-P. Morency, "Multimodal machine learning: A survey and taxonomy," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 41, no. 2, pp. 423–443, 2019.
[45] P. P. Liang, A. Zadeh, and L.-P. Morency, "Foundations & trends in multimodal machine learning: Principles, challenges, and open questions," *ACM Comput. Surv.*, vol. 56, no. 10, pp. 1–42, 2024.
[46] O. Khatib, "A unified approach for motion and force control of robot manipulators: The operational space formulation," *IEEE J. Robot. Autom.*, vol. 3, no. 1, pp. 43–53, 1987.
[47] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, 1949.
[48] X. Li *et al.*, "Evaluating real-world robot manipulation policies in simulation," in *Proc. Conf. Robot Learn. (CoRL)*, Munich, Germany, 2024, pp. 1–24.
[49] M. J. Kim *et al.*, "OpenVLA: An open-source vision-language-action model," in *Proc. Conf. Robot Learn. (CoRL)*, Munich, Germany, 2024, pp. 1–35.
[50] D. Ghosh *et al.*, "Octo: An open-source generalist robot policy," in *Proc. Robot. Sci. Syst. (RSS)*, Delft, Netherlands, 2024, pp. 1–13.

Ching-Chun Chang received the PhD in Computer Science from the University of Warwick, UK, in 2019. He is currently a Project Assistant Professor with the National Institute of Informatics, Japan. He participated in a short-term scientific mission supported by European Cooperation in Science and Technology Actions at the Faculty of Computer Science, Otto von Guericke University of Magdeburg, Germany, in 2016. He was granted the Marie-Curie fellowship and participated in a research and innovation staff exchange scheme supported by Marie Sk lodowska-Curie Actions at the Department of Electrical and Computer Engineering, New Jersey Institute of Technology, USA, in 2017. He was a Visiting Scholar with the School of Computer and Mathematics, Charles Sturt University, Australia, in 2018, and with the School of Information Technology, Deakin University, Australia, in 2019. He was a Research Fellow with the Department of Electronic Engineering, Tsinghua University, China, in 2020. His research interests include artificial intelligence, biometrics, cryptography, cybersecurity, evolutionary computation, forensics, information theory, steganography, and watermarking.



Yijie Lin received the BS degree in Computer Science and Information Engineering from National Pingtung University, Taiwan, in 2022. He is currently pursuing a PhD degree with the Department of Information Engineering and Computer Science, Feng Chia University, Taiwan. His research interests include artificial intelligence, computer vision, cybersecurity, steganography, and watermarking.

Isao Echizen received BS, MS, and DE degrees from the Tokyo Institute of Technology, Japan, in 1995, 1997 and 2003, respectively. He joined Hitachi, Ltd. in 1997 and until 2007 was a Research Engineer in the company's systems development laboratory. He is currently a Director and Professor of the Information and Society Research Division, as well as a Director of the Global Research Center for Synthetic Media, at the National Institute of Informatics; a Professor in the Department of Information and Communication Engineering, Graduate School of Information Science and Technology, the University of Tokyo; and a Professor in the Graduate Institute for Advanced Studies, the Graduate University For Advanced Studies (SOKENDAI), Japan. He was a Visiting Professor at the Tsuda University, Japan; at the University of Freiburg, Germany; and at the University of Halle-Wittenberg, Germany. He is currently engaged in research on multimedia security and multimedia forensics, serving as a Research Director in the CREST FakeMedia project, Japan Science and Technology Agency (JST). He received the Best Paper Award from the IPSJ in 2005 and 2014; the Fujio Frontier Award and the Image Electronics Technology Award in 2010; the One of the Best Papers Award from the Information Security and Privacy Conference in 2011; the IPSJ Nagao Special Researcher Award in 2011; the DOCOMO Mobile Science Award in 2014; the Information Security Cultural Award in 2016; the IEEE Workshop on Information Forensics and Security Best Paper Award in 2017; and the Best Paper Award from the IEICE in 2023. He was a Member of the Information Forensics and Security Technical Committee of the IEEE Signal Processing Society. He is an IEICE Fellow, IEEE Senior Member, and Japanese Representative on IFIP TC11 (Security and Privacy Protection in Information Processing Systems), Member-at-Large of the Board of Governors of APSIPA, and Editorial Board Member of the *IEEE Transactions on Dependable and Secure Computing*, *EURASIP Journal on Image and Video Processing*, and *Elsevier Journal of Information Security and Applications*