

Haptic-Based User Authentication for Tele-robotic System

Rongyu Yu¹, Kan Chen², Zeyu Deng³, Chen Wang³, Burak Kizilkaya², Emma Li²

Abstract—Tele-operated robots rely on real-time user behavior mapping for remote tasks, but ensuring secure authentication remains a challenge. Traditional methods, such as passwords and static biometrics, are vulnerable to spoofing and replay attacks, particularly in high-stakes, continuous interactions. This paper presents a novel anti-spoofing and anti-replay authentication approach that leverages distinctive user behavioral features extracted from haptic feedback during human–robot interactions. To evaluate our authentication approach, we collected a time-series force feedback dataset from 15 participants performing seven distinct tasks. We then developed a transformer-based deep learning model to extract temporal features from the haptic signals. By analyzing user-specific force dynamics, our method achieves over 90% accuracy in both user identification and task classification, demonstrating its potential for enhancing access control and identity assurance in tele-robotic systems.

Index Terms—User authentication, Behavioral biometrics, Haptic-based biometrics, Human-robot interaction, Cyber physical security

I. INTRODUCTION

Cognitive robotics has made significant progress in recent years, such as deep learning-based perception for real-time object recognition and grasping [1], as well as reinforcement learning techniques [2] enabling robots to autonomously acquire complex motor skills. However, current fully autonomous systems still struggle to replicate nuanced, human-like decision-making and dexterous manipulation, that are particularly essential for many mission-critical tasks such as remote surgery [3] and hazardous material handling [4], where expert human judgment and direct control are crucial for ensuring safety and security [5].

At the same time, as robots become more integrated into our daily lives, robust remote access control and user authentication are essential to prevent unauthorized access, secure sensitive data, and guard against potential cyber threats. Weak security measures pose a significant risk, allowing adversary attackers to manipulate operations, steal information, or

disrupt services, thereby highlighting the need for stringent safeguards and secure interfaces in both networked robotic systems and human–robot interactions.

Haptic feedback play a crucial role in improving user interaction with robotic systems by providing tactile responses that enhance control precision, enabling operators to perceive physical phenomena such as force, vibration, and impact in both virtual and remote environments. This real-time tactile perception not only heightens immersion and realism, but also provides critical cues for precise manipulation, enhanced safety, and efficient task execution.

Cyber-Physical System (CPS) [6] merge computing, networking, and physical components to enable real-time monitoring and control across both digital and physical domains. By seamlessly linking devices, sensors, and human operators, CPS incorporate advanced feedback loops that significantly enhance processes such as human–robot interactions, providing lower-latency and higher-fidelity data [7]. In the field of robotics, digital twins leverage these feedback loops to enable more precise coordination between operators and robots, support complex decision-making, and facilitate tasks such as remote surgery or autonomous navigation. However, this high degree of connectivity also increases security risks [8], as malicious actors may exploit vulnerable communication channels or compromised devices to manipulate system behavior. Consequently, CPS require robust user authentication and access-control mechanisms to block unauthorized access, protect data integrity, and ensure safe, reliable operation.

Traditional credential-based authentication methods for robotic security are often vulnerable to phishing, brute-force attacks, and shoulder surfing. For example, passwords can be easily stolen, compromised, or forgotten [9]. By contrast, biometric techniques offer stronger protection against spoofing by leveraging unique human physical traits, which are inherently more difficult to replicate or forge.

These approaches can be broadly categorized into physiological and behavioral biometrics. Physiological biometrics utilize personal physical attributes such as fingerprints, facial features, and iris patterns. Behavioral biometrics, on the other hand, analyze distinctive human behavioral patterns such as typing rhythms, signature dynamics, and gait. Behavioral biometrics are challenging to replicate and offer the additional benefit of enabling continuous authentication [10].

Haptic-based behavioral biometrics provide a dynamic, hard-to-forge, and context-sensitive authentication technique by utilizing each individual’s distinct force dynamics [11]. Generally, this approach is applied as the additional layer of security (two-factor authentication) to traditional credential-

This work involved human subjects in its research. Approval of all ethical and experimental procedures and protocols was granted by the University Ethics Committee of the University of Glasgow under Application 300230225 and performed in line with European General Data Protection Regulation (GDPR).

¹Rongyu Yu is with James Watt School of Engineering, University of Glasgow, Glasgow, G12 8QQ, UK 2658366y@student.gla.ac.uk, burak.kizilkaya@glasgow.ac.uk

²Kan Chen, Burak Kizilkaya, Emma Li are with the School of Computing Science, University of Glasgow, Glasgow, G12 8RZ, UK liying.li@glasgow.ac.uk, k.chen.1@research.gla.ac.uk

³Zeyu Deng and Chen Wang are with the Computer Science Department, Southern Methodist University, Dallas, TX, United States zeyud@smu.edu, cwang6@smu.edu

based authentication techniques, such as PINs [12], [13], signatures [14], or pattern locks [15], which are often compromised through “shoulder surfing,” where attackers observe passwords without the user’s consent.

In [12], authors introduce an eyes-free mobile authentication method using random starting digits, vertical swipe gestures, and morse code vibration feedback, validated via a 20-participant user study and a 15-participant shoulder-surfing experiment. In [13], Bianchi et al. propose the Secure Haptic Keypad (SHK), a tactile-based PIN entry system that mitigates shoulder-surfing attacks by encoding each digit as a unique vibration pattern. User studies show that SHK provides enhanced security with minimal impact on input speed and accuracy. In [14], the authors leverage a 6-DOF Phantom Omni Device to record multi-dimensional input data (position, velocity, forces, pen orientation) and uses a Dynamic Time Warping (DTW) to extract features for an artificial neural network, achieving high accuracy, resisting forgery, and remaining user-friendly. Furthermore, in [15], the authors presents a dial-based interface for public terminals (e.g., ATMs) that employs tactons (structured vibration patterns) to improve PIN entry efficiency and reduce errors.

Furthermore, earlier work [16] has demonstrated that each user exhibits a distinctive and identifiable motion pattern when teleoperating a robotic system, pointing to a potential behavioral-biometric solution for robotic security. Meanwhile, robot learning from demonstration (LfD) is a well-established method that allows robots to learn to replicate human behaviors by observing demonstrations. Our previous research also explored how robots can learn user-specific keystroke dynamics [17]. Building on these insights, it is promising to incorporate user-specific force dynamics in future studies, enabling robots to capture the specialized behaviors of different task experts.

In summary, existing haptic biometric methods reinforce traditional authentication by leveraging each user’s unique force dynamics, offering an additional layer of security. This approach provides robust defense against shoulder-surfing attacks and shows strong potential to improve usability, accuracy, and resilience against impersonation threats. However, as tele-operated robotic arms become more common in daily life, the need for robust, continuous authentication during teleoperation grows. Current solutions rarely apply behavioral biometrics throughout the robotic manipulation process. To address this gap, we propose a novel, haptic-based user authentication system for tele-robotic applications, which uses user-specific force feedback patterns to provide continuous, reliable verification. To our knowledge, this is the first work demonstrating the feasibility of using haptic biometrics to authenticate tele-operators.

The main contributions can be summarized as follows.

- 1) In this paper, we develop a haptic-based user authentication system for tele-robotic applications. We show that force feedback inherently carries personal information about the operator in human-machine interaction, especially under remote control.
- 2) We conducted a large-scale user data collection, gathering 120 samples across 7 tasks from 15 participants.

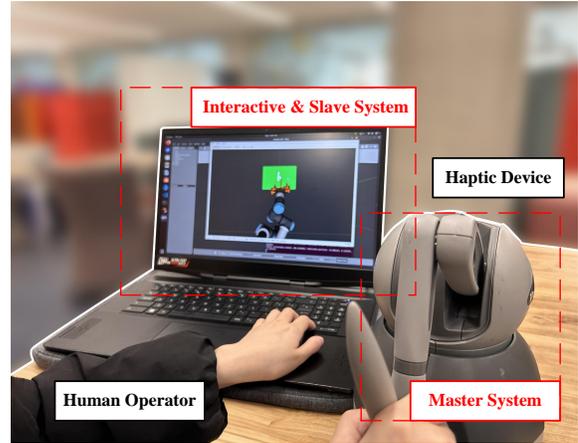


Fig. 1. Overview of the virtual teleoperation system illustrating the four main components. A human operator (left) manipulates the master systems via the haptic device (right), which provides haptic force feedback. These inputs are transmitted to the interactive and slave systems displayed on the laptop, enabling intuitive remote control and interaction.

Our findings demonstrate that haptic signals during robot teleoperation can be leveraged for user identification and task classification.

- 3) We propose a transformer-based deep learning algorithm that extracts time-series features from haptic signals for user identification and task classification, using the data set we collected.
- 4) Finally, we validate our approach by collecting data from 15 participants using a virtual motion-controlled robotic arm platform. Each participant performs seven tasks by writing the letters *a*, *b*, *c*, *d*, *e*, *f*, *g* on a plate. We then evaluate both the raw and filtered force data, demonstrating that haptic signals can achieve over 90% accuracy in user identification and task classification.

The remainder of this paper is structured as follows. In Section II, we describe the system architecture and experimental procedure. Section III introduces the design and implementation of our user authentication mechanism, including the data processing of haptic signals and details of model training. Section IV presents the results and provides a thorough analysis. Finally, in Section V, we conclude the study by summarizing the key findings and discussing their implications for future research.

II. SYSTEM ARCHITECTURE AND EXPERIMENTAL PROCEDURE

A. System Overview

The experimental system in this study comprises both hardware and software components that together enable precise simulation and data recording of human-robot interactions. As illustrated in Fig. 1, a human operator interacts with a virtual robot using a haptic device controller, which provides real-time force feedback. These interactions are transmitted over a virtual tele-robotic system, facilitating intuitive remote control and operation.

B. Software Components

In our system, the robotic virtual environment and control infrastructure are built using the Robot Operating System (ROS) Noetic MoveIt framework [18]. This platform integrates motion planning, kinematics solving, collision detection, and visualization into a unified architecture. We employ Gazebo [19] rendering engine to construct the virtual environment, as it offers relatively low CPU latency and delivers accurate sensing capabilities along with real-time haptic force feedback. We will use RViz [20] for both object visualization and handwritten letter visualization.

1) *Virtual Environment and Update Rates*: The Gazebo simulation environment is configured with a 250 Hz update rate for both the virtual world and the robot state controller, ensuring responsive control and seamless interaction.

All data streams including raw data from Force-Torque Sensor (TF) and filtered force data are recorded at 250 Hz to ensure consistency. By aligning each component (simulation, controller, and data recording) to the same update frequency, we achieve stable control cycles and synchronized sensor data acquisition.

C. Haptic Rendering

We employ a simple haptic rendering mechanism that reads and scales raw force data from TF. When the pen tip contacts the plate, TF collision detection is triggered. An Exponential Moving Average Filter (EMAF) with a smoothing constant $\alpha = 0.001$ is then applied to update the force, and the smoothed force is provided to the user as haptic feedback, ensuring a seamless and responsive virtual interaction. If the detected raw force falls below a preset threshold (for example, when the user’s pen tip leaves the platform), the force quickly decays.

1) *Hardware Components*: We employ the *Touch Haptic* device (also known as the *Geomagic Touch*) as the human input interface. This controller provides six degrees of freedom (DoF) for tracking the spatial position and orientation of the user’s hand, enabling intuitive manipulation of virtual robotic arms in the world space. It also delivers three-dimensional force feedback for interactive and natural control. Additionally, we use an MSI GS77 laptop configured with a 12th Gen Intel i9-12900H processor to simulate the virtual environment and robot, as well as to run an interactive master–slave system for real-time robot manipulation via the haptic device.

D. Experimental Procedure and Data Collection

The hand movements of the participants were directly assigned to the end effector of the robotic arm. Data collected from 15 volunteers produced a total of $120 \times 7 \times 15 = 12,600$ samples. Data collection was organized into seven sessions. A short break followed each session, and participants could request additional pauses at any time. All trials were carried out in the school library under natural conditions of ambient.

The force data in the x -, y -, and z -directions, along with the corresponding virtual timestamps, were saved to a Comma-Separated Values (CSV) file, anonymized, and stored in compliance with General Data Protection Regulation (GDPR)

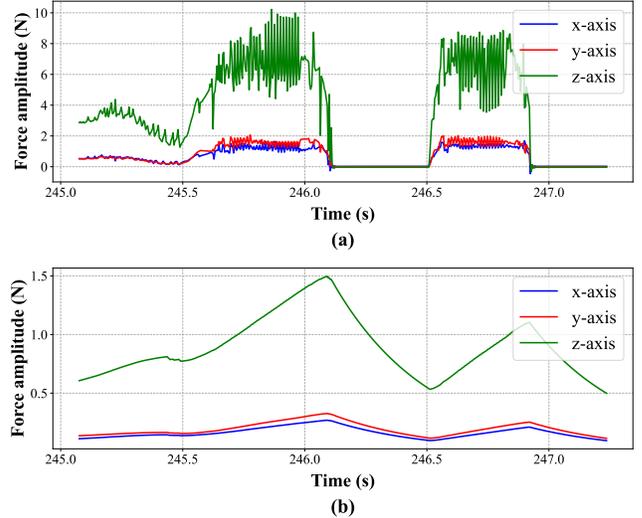


Fig. 2. Illustrations of the force signals (a) before filtering and (b) after applying a EMAF across the x-axis, y-axis, and z-axis. The raw signals in (a) capture the full range of force fluctuations, while (b) shows the smoothed force profiles highlighting the major variations over time.

requirements. To preserve realistic interaction scenarios, we deliberately applied no noise filtering or other preprocessing to the haptic data. All subsequent experiments and analyses relied on this unfiltered dataset, ensuring that the results are representative of practical application environments.

As shown in Fig 2, during the experiment, **two types of force data** were recorded:

- 1) **Raw Force Data**: The force data were recorded from the force torque sensor of Universal Robots UR3e (UR3e).
- 2) **Filtered Force Data**: The data were collected by applying an EMAF to the raw force data.

All participants signed informed consent forms and all collected data, including personal information, were processed in strict accordance with the university’s ethics regulations. To protect participant privacy, all identifiers were anonymized before storage and data was kept on secure, access-controlled servers. Biometric identifiers or personally traceable metadata were not retained. Participants were explicitly informed of the purpose of data collection, the scope of data usage, and their right to withdraw at any time without penalty. Furthermore, the study design followed the GDPR principles of data minimization and purpose limitation, ensuring that only the data strictly necessary for the research objectives were collected and retained.

III. USER AUTHENTICATION DESIGN

A. Data Processing

1) *Feature Extraction*: We record three-axis force measurements $\{F_x(t), F_y(t), F_z(t)\}$ at a sampling rate $S = 250$ Hz. For each pair of consecutive time samples, we compute higher-order force features by subtracting adjacent sample values and multiplying by S . Specifically, we derive the instantaneous force difference, force velocity, force acceleration, and force

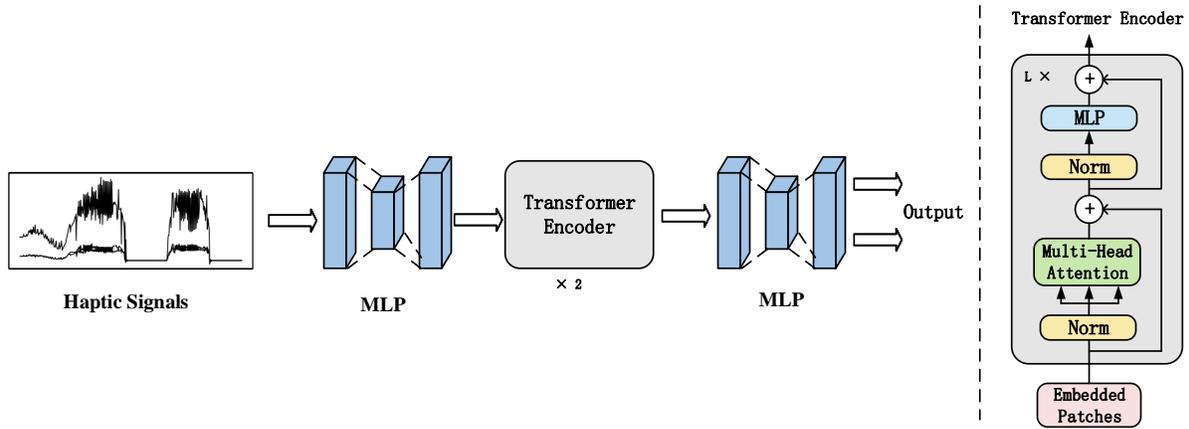


Fig. 3. An overview of the proposed transformer-based model.

jerk. As summarized in Table I, each pair of adjacent data points thus yields 13 derived features.

B. Model Training

1) *Model Architecture*: As shown in Figure 3, we employ a two-layer Transformer-based model to classify haptic signals. The Transformer encoder is composed of multiple stacked encoder layers, each consisting of two main components: Multi-Head Self-Attention (MHSA) and Feed-Forward Neural Network (FFNN). In the multi-head self-attention mechanism, the input haptic signal sequence is first mapped into *Query*, *Key*, and *Value* vectors. By computing attention weights among different time steps or features in the sequence, the relevant information is aggregated, enabling the model to capture critical temporal and feature dependencies in the haptic data. Subsequently, the feed-forward network is applied independently to each position in the sequence and contains two fully connected layers with a ReLU activation in between. The first layer projects the features into a higher-dimensional space, and the second layer maps them back to the original model dimension.

2) *Training Procedure*: In this study, we trained separate models for task classification and user identification. We begin by randomly shuffling the entire dataset. Then, for each user performing a given task, we split their data into 100 samples for training and 20 samples for testing.

TABLE I
FORCE VECTOR BASED FEATURE EXTRACTION

Feature	Notation / Definition
Force Difference	$\Delta \mathbf{F}(t) = \ \mathbf{F}(t+1) - \mathbf{F}(t)\ $
Velocity	$\dot{\mathbf{F}}(t) = (\dot{F}_x(t), \dot{F}_y(t), \dot{F}_z(t))^T$
Velocity Norm	$\ \dot{\mathbf{F}}(t)\ = \sqrt{\dot{F}_x^2(t) + \dot{F}_y^2(t) + \dot{F}_z^2(t)}$
Acceleration	$\ddot{\mathbf{F}}(t) = (\ddot{F}_x(t), \ddot{F}_y(t), \ddot{F}_z(t))^T$
Acceleration Norm	$\ \ddot{\mathbf{F}}(t)\ = \sqrt{\ddot{F}_x^2(t) + \ddot{F}_y^2(t) + \ddot{F}_z^2(t)}$
Jerk	$\overset{\cdot}{\ddot{\mathbf{F}}}(t) = (\overset{\cdot}{\ddot{F}}_x(t), \overset{\cdot}{\ddot{F}}_y(t), \overset{\cdot}{\ddot{F}}_z(t))^T$
Jerk Norm	$\ \overset{\cdot}{\ddot{\mathbf{F}}}(t)\ = \sqrt{\overset{\cdot}{\ddot{F}}_x^2(t) + \overset{\cdot}{\ddot{F}}_y^2(t) + \overset{\cdot}{\ddot{F}}_z^2(t)}$

For user identification, we trained 7 task-specific models, one per letter, where each user provides 100 training samples (1,500 total) and 20 testing samples (300 total) for that letter. For task classification, we trained 15 user-specific models, each with 100 training samples per letter (700 total), and then tested them on 7 letters, with 20 samples per letter (140 total).

3) *Implementation Details*: For user identification and task classification, we adopt slightly different approaches to process the force data. For task classification, we downsample the extracted force features to a fixed length of 64. By contrast, for user identification, we downsample each sequence to a length of 512, providing a richer temporal context that helps distinguish subtle individual-specific force signatures. Our model is implemented using PyTorch and PyTorch Lightning for efficient training, with the Adam optimizer at a learning rate of 10^{-4} and a cosine annealing scheduler to mitigate overfitting, all run for 100 epochs for both user identification and task classification purposes. Both training tasks use a batch size of 16. Additionally, each Transformer block features a hidden dimension of 256 and 16 attention heads, along with a feed-forward sub-block of dimension 256. Finally, a two-layer Transformer encoder is employed to effectively extract temporal features from the haptic signals.

C. Performance Metrics

In this study, our evaluation criteria for user identification and task classification performance are Accuracy (ACC) and Precision (Prec), which measure the model's ability to correctly identify users or tasks.

- 1) **Accuracy**: Accuracy is an overall indicator of a model's correctness, calculated as the ratio of accurately classified instances to the total number of instances.
- 2) **Precision**: For a particular user, precision indicates the proportion of instances predicted to belong to that user which actually belong to that user.

IV. PERFORMANCE EVALUATION

A. Task classification

In this section, we evaluate the performance of task classification using haptic signals while the human operator performs

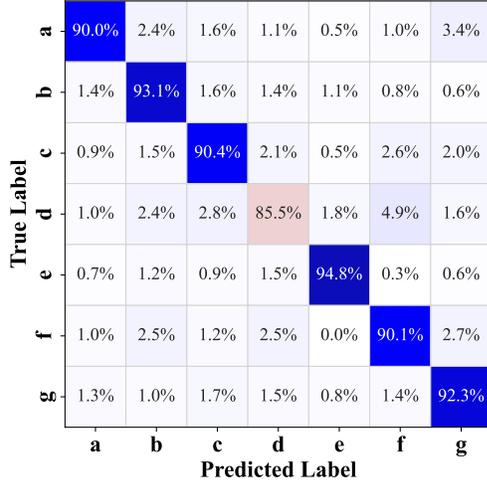


Fig. 4. Confusion matrix of task classification (raw force).

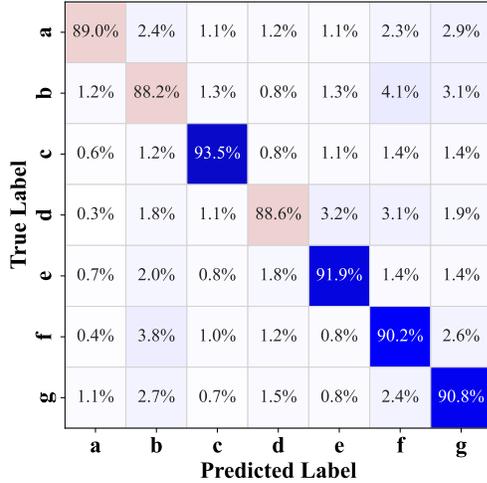


Fig. 5. Confusion matrix of task classification (filtered force).

different tasks. As demonstrated in our experimental results, both the raw force data and the filtered force data achieve high accuracy, exceeding 90%.

This finding demonstrates that when a user manipulates a robotic arm, the force signals not only reflect the user's intent but also capture the specific characteristics of the task at hand. Consequently, these haptic signals can serve as a reliable input for task classification in human-robot collaboration settings. However, given the potential privacy and security implications arising from the leakage of such data, it is crucial to ensure robust protection of these haptic signals.

B. User Identification

In this section, we evaluate user identification performance using haptic signals obtained as the human operator performs various tasks.

As shown in Fig. 6, the raw force data yields high user identification rates (over 90%) for all users. Meanwhile, the

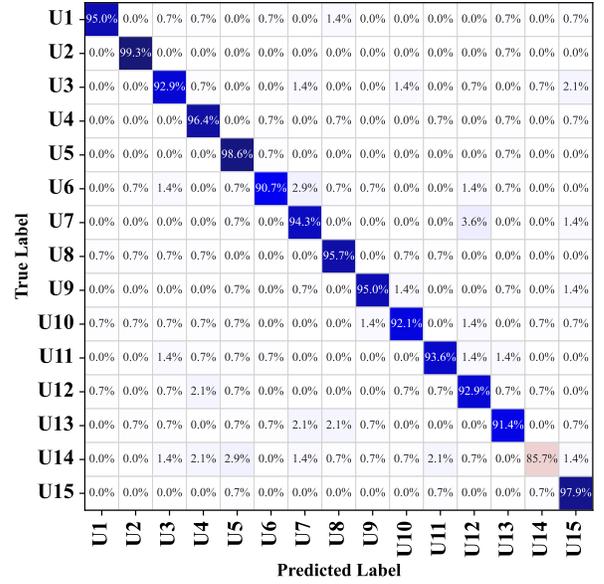


Fig. 6. Confusion matrix of user identification (raw force).

filtered force data (Fig. 7) achieves more than 90% for every user except U3.

These results demonstrate that when an operator remotely controls a robotic arm, the forces they apply exhibit unique, individual force signatures. Consequently, force-based signals offer a promising approach for user identification in human-machine interaction. In effect, the robotic system captures and reflects human behavior through these force measurements, embedding the operator's distinctive behavioral patterns into the robot's behavior.

However, the feasibility to identify users based on their force signatures also introduces security and privacy concerns. Because such force data could be used to track or profile individuals, it is essential to establish robust data protection measures, such as anonymizing force signals, employing secure storage and transmission protocols to safeguard the privacy of operators.

As shown in Fig. 8, we provide the average precision of each model across seven tasks. For user identification performance, using the raw force for recognition yields accuracies ranging from 90.27% to 97.21%, with an average of about 93.46%. In comparison, using filtered force yields accuracies from 88.46% to 98.58%, also averaging around 92.89%.

These results demonstrate consistently high recognition accuracy for user identification, indicating that our method effectively leverages force-based haptic signals, which exhibit distinctive user uniqueness.

C. Impact of Training Data Size

In order to investigate how varying the training data size affects task classification performance, we incrementally increase the number of training instances from 5 to 100 in steps of 5. As shown in Fig. 10, we present the average accuracy across different users using raw force data. Our results demonstrate that accurate task classification is achievable

True Label \ Predicted Label	U1	U2	U3	U4	U5	U6	U7	U8	U9	U10	U11	U12	U13	U14	U15
U1	95.0%	0.0%	0.0%	1.4%	0.0%	1.4%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.7%	0.7%
U2	2.1%	94.3%	0.0%	0.0%	0.7%	0.0%	1.4%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.7%
U3	0.0%	0.7%	89.3%	0.0%	0.0%	0.7%	2.9%	0.7%	0.0%	0.7%	1.4%	0.0%	0.0%	2.1%	1.4%
U4	0.0%	0.7%	0.7%	88.6%	0.7%	1.4%	0.7%	2.9%	0.0%	0.0%	1.4%	1.4%	0.0%	1.4%	0.0%
U5	0.0%	0.7%	0.0%	0.0%	94.3%	0.7%	0.0%	0.0%	0.0%	2.1%	0.7%	0.0%	0.7%	0.7%	0.0%
U6	0.7%	0.0%	0.0%	0.0%	0.0%	97.1%	0.7%	0.0%	0.0%	0.0%	0.7%	0.0%	0.0%	0.7%	0.0%
U7	0.7%	0.0%	0.7%	0.0%	0.0%	1.4%	94.3%	0.7%	0.0%	0.0%	0.7%	0.0%	1.4%	0.0%	0.0%
U8	0.0%	0.7%	0.0%	0.0%	0.0%	2.1%	0.7%	90.7%	0.0%	0.7%	3.6%	0.7%	0.0%	0.7%	0.0%
U9	0.0%	0.0%	0.0%	0.0%	0.0%	2.1%	0.0%	0.7%	94.3%	0.0%	0.7%	0.7%	0.7%	0.0%	0.7%
U10	0.0%	0.7%	1.4%	0.7%	1.4%	0.0%	0.7%	0.7%	0.0%	91.4%	0.7%	0.0%	0.7%	0.7%	0.7%
U11	1.4%	0.0%	0.7%	0.0%	0.0%	0.0%	0.0%	0.7%	0.0%	1.4%	95.0%	0.0%	0.0%	0.7%	0.0%
U12	0.0%	0.0%	0.0%	0.0%	0.7%	0.0%	0.7%	0.0%	0.0%	0.0%	0.7%	97.9%	0.0%	0.0%	0.0%
U13	2.1%	1.4%	0.0%	1.4%	0.7%	1.4%	2.1%	1.4%	0.0%	0.7%	1.4%	0.7%	85.7%	0.7%	0.0%
U14	0.0%	0.7%	0.0%	0.7%	0.0%	0.7%	0.7%	0.0%	0.7%	0.0%	1.4%	0.0%	0.7%	94.3%	0.0%
U15	0.7%	0.0%	0.7%	0.0%	0.7%	0.0%	0.0%	0.0%	0.7%	0.0%	0.0%	0.0%	0.0%	0.0%	97.1%

Fig. 7. Confusion matrix of user identification (filtered force).

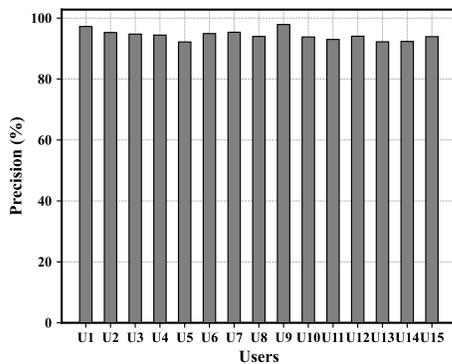


Fig. 8. Performance user identification (raw force).

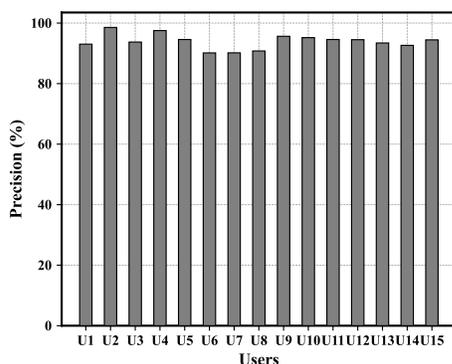


Fig. 9. Performance of user identification (filtered force).

using haptic signals even with a limited amount of training data. Furthermore, the performance gradually improves as the training set size increases, ultimately exceeding 94%.

We also explore task classification performance using fil-

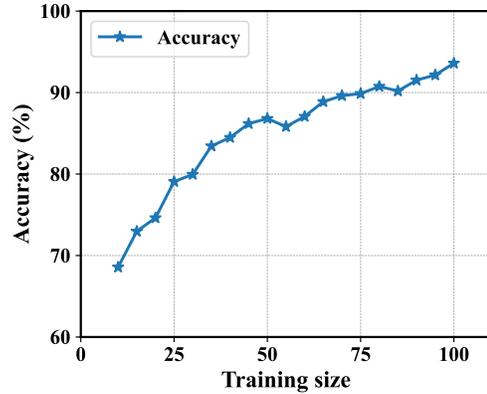


Fig. 10. Performance of task classification under different training size (raw force).

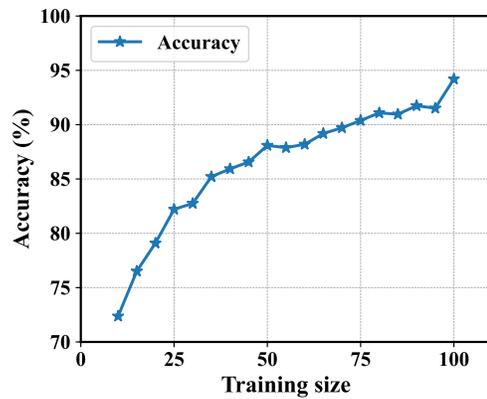


Fig. 11. Performance of task classification under different training size (filtered force).

tered force data. As illustrated in Fig. 11, with just 5 training samples, the classification accuracy is around 72%. Furthermore, this accuracy continues to improve as the training set size grows and reaches 95%.

V. CONCLUSION

This paper explores the performance of haptic signals for both user identification and task classification in a telerobotic human-robot interaction scenario. Our results indicate that force feedback inherently carries personal information about the operator, particularly in remote-control settings. Moreover, by employing a two-layer Transformer model architecture, we achieve over 90% accuracy in both user identification and task classification. Our findings indicate that force feedback data, collected while a human operator controls a robotic arm, is inherently identifiable, raising significant security and privacy concerns. Consequently, our future work will focus on developing privacy-preserving methods to anonymize user data, investigating how to balance usability with robust personal information protection.

REFERENCES

- [1] H. Yin, A. Varava, and D. Kragic, "Modeling, learning, perception, and control methods for deformable object manipulation," *Science Robotics*, vol. 6, no. 54, p. eabd8803, 2021.
- [2] J. Kober, J. A. Bagnell, and J. Peters, "Reinforcement learning in robotics: A survey," *The International Journal of Robotics Research*, vol. 32, no. 11, pp. 1238–1274, 2013.
- [3] G. H. Ballantyne, "Robotic surgery, telerobotic surgery, telepresence, and telementoring," *Surgical Endoscopy and Other Interventional Techniques*, vol. 16, pp. 1389–1402, 2002.
- [4] O. Tokatli, P. Das, R. Nath, L. Pangione, A. Altobelli, G. Burroughes, E. T. Jonasson, M. F. Turner, and R. Skilton, "Robot-assisted glovebox teleoperation for nuclear industry," *Robotics*, vol. 10, no. 3, p. 85, 2021.
- [5] K. Darvish, L. Penco, J. Ramos, R. Cisneros, J. Pratt, E. Yoshida, S. Ivaldi, and D. Pucci, "Teleoperation of humanoid robots: A survey," *IEEE Transactions on Robotics*, vol. 39, no. 3, pp. 1706–1727, 2023.
- [6] R. Baheti and H. Gill, "Cyber-physical systems," *The impact of control technology*, vol. 12, no. 1, pp. 161–166, 2011.
- [7] G. Schirner, D. Erdogmus, K. Chowdhury, and T. Padir, "The future of human-in-the-loop cyber-physical systems," *Computer*, vol. 46, no. 1, pp. 36–45, 2013.
- [8] A. Khalid, P. Kirisci, Z. H. Khan, Z. Ghairi, K.-D. Thoben, and J. Pannek, "Security framework for industrial collaborative robotic cyber-physical systems," *Computers in Industry*, vol. 97, pp. 132–145, 2018.
- [9] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," in *2012 IEEE symposium on security and privacy*. IEEE, 2012, pp. 553–567.
- [10] A. K. Jain, A. Ross, and S. Pankanti, "Biometrics: a tool for information security," *IEEE transactions on information forensics and security*, vol. 1, no. 2, pp. 125–143, 2006.
- [11] A. El Saddik, M. Orozco, Y. Asfaw, S. Shirmohammadi, and A. Adler, "A novel biometric system for identification and verification of haptic users," *IEEE Transactions on Instrumentation and Measurement*, vol. 56, no. 3, pp. 895–906, 2007.
- [12] P. V. Bhole, Z. Li, S. Bokolia, T. Oh, G. W. Tigwell, and R. L. Peiris, "Haptic2fa: Haptics-based accessible two-factor authentication for blind and low vision people," *Proceedings of the ACM on Human-Computer Interaction*, vol. 8, no. MHCI, pp. 1–20, 2024.
- [13] A. Bianchi, I. Oakley, and D. S. Kwon, "The secure haptic keypad: a tactile password system," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2010, pp. 1089–1092.
- [14] G. Dhandapani, J. Ferguson, and E. Freeman, "Hapticlock: Eyes-free authentication for mobile devices," in *Proceedings of the 2021 International Conference on Multimodal Interaction*, 2021, pp. 195–202.
- [15] J. Yan, K. Huang, T. Bonaci, and H. J. Chizeck, "Haptic passwords," in *2015 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*. IEEE, 2015, pp. 1194–1199.
- [16] L. Huang, Z. Meng, Z. Deng, C. Wang, L. Li, and G. Zhao, "Toward verifying the user of motion-controlled robotic arm systems via the robot behavior," *IEEE Internet of Things Journal*, vol. 9, no. 22, pp. 22422–22433, 2021.
- [17] R. Yu, B. Kizilkaya, Z. Meng, E. Li, and P. Zhao, "Robot adversarial attack on keystroke dynamics based user authentication system," *IEEE Robotics and Automation Letters*, pp. 1–8, 2025.
- [18] ROS Wiki, "RViz," <http://wiki.ros.org/rviz>, accessed March 20, 2025.
- [19] "Classic gazebo official website," <https://classic.gazebo.org/>, accessed: 2025-03-23.
- [20] "Rviz (ros wiki)," <http://wiki.ros.org/rviz>, accessed: 2025-03-23.