Poster: Rhythm Tap: Inclusive Personal Authentication Method Based on Rhythmic Variation

Yuri Takase*, Yuto Toshikawa*, Kazuki Nomoto*, Ryo Iijima¶*, Masataka Kakinouchi†, Tatsuya Mori*‡§,
*Waseda University †Tsukuba University of Technology ‡RIKEN §NICT ¶AIST

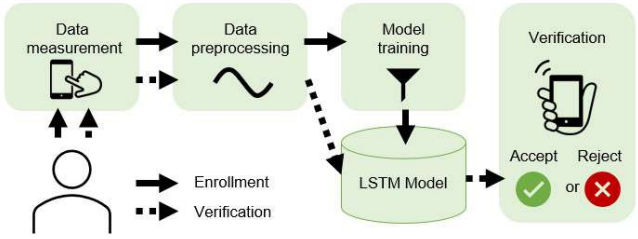


Fig. 1. Overview of the RHYTHM TAP workflow.

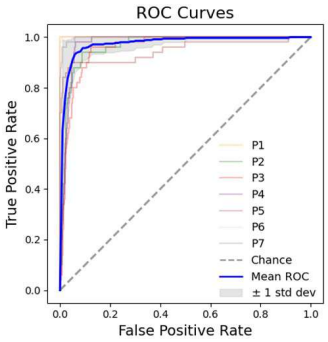


Fig. 2. ROC curve of the authentication model tested with visually impaired participants.

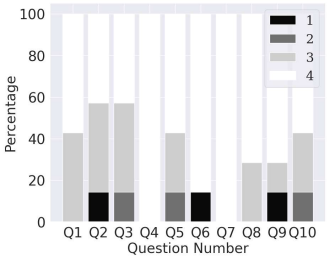


Fig. 3. Distribution of responses to the SUS questionnaire for the group with visual impairment.

***Abstract*—This study introduces RHYTHM TAP, an authentication system leveraging rhythmic tapping patterns as a personalized biometric identifier. Designed to enhance usability and accessibility, particularly for visually impaired users, RHYTHM TAP bridges gaps in existing authentication technologies. Implemented on the Android platform, the system was evaluated through a user study, demonstrating high accuracy, usability, and security. These results highlight RHYTHM TAP's potential as a robust and inclusive alternative for mobile authentication.**

I. INTRODUCTION

Mobile devices are indispensable for managing personal information, requiring secure and accessible authentication methods. However, traditional authentication mechanisms, such as passcodes, fingerprint recognition, and pattern locks, often fail to address the unique needs of visually impaired users, who face challenges like precise positioning and extended input times. This lack of accessibility restricts the adoption of these methods among visually impaired users.

RHYTHM TAP addresses these challenges by introducing rhythmic tapping patterns as a behavioral biometric. This novel method capitalizes on natural differences in rhythm perception and synchronization to provide an inclusive, user-friendly, and secure authentication alternative. The system complements existing security measures, enhancing their usability for both visually impaired users.

II. METHODOLOGY

The workflow of RHYTHM TAP, as shown in Figure 1, consists of two phases: enrollment and verification. The user-generated rhythmic tapping patterns are collected using the smartphone's built-in accelerometer. Once collected, the data undergoes pre-processing, such as normalizing the sequence length before being fed into the authentication model. The model is a deep learning architecture based on Long Short-Term Memory (LSTM) networks that is trained using data from the enrollment phase. During the verification phase, the system measures the user's taps, processes the data, and feeds it into the authentication model. This model then evaluates whether the input matches the registered pattern and provides auditory feedback to the user regarding the authentication outcome. The system was implemented as a proof-of-concept (PoC) on Android, with the backend processing handled by a PC server.

TABLE I
AVERAGE AUTHENTICATION ACCURACY PER USER.

	First 5 trials	Total 50 trials
Visually impaired	0.992	0.897
Sighted	0.986	0.952

The system was evaluated with 17 participants (7 visually impaired, 10 sighted) aged 19–24. Participants performed rhythmic tapping on various smartphone surfaces (screen, back, side) to test its accuracy, usability, and security. Participants created their rhythms by tapping along to a song of their choice, providing a high degree of personalization. Visually impaired users utilized accessibility features such as screen readers to navigate the system, ensuring inclusivity during the study. User satisfaction was assessed using the System Usability Scale (SUS) [1].

III. EVALUATION

Figure 2 presents the Receiver Operating Characteristic (ROC) curve for the LSTM model. The evaluation is based on

TABLE II

CORRELATION BETWEEN RHYTHM PATTERNS CREATED BY TARGET USERS AND AVERAGE SUCCESS RATES FOR THREE ATTACK SCENARIOS: BRUTE FORCE (r_b), VISUAL IMPERSONATION (r_v), AND AUDIOVISUAL IMPERSONATION (r_{av}) ATTACKS. VARIABLES ARE: T (RHYTHM LENGTH IN SECONDS), m (NUMBER OF SMARTPHONE SURFACES USED FOR TAPPING), WITH RESULTS SHOWN FOR 5 AND 50 ATTACK ATTEMPTS.

Target	T	m	$r_b(5)$	$r_v(5)$	$r_{av}(5)$	$r_b(50)$	$r_v(50)$	$r_{av}(50)$
P1	7	1	0.000	0.133	0.533	0.017	0.750	0.922
P2	2	1	0.000	1.000	1.000	0.028	0.961	1.000
P3	5	2	0.000	0.000	0.033	0.000	0.094	0.306
P6	5	2	0.000	0.000	0.000	0.000	0.022	0.061
P7	6	1	0.000	0.000	0.067	0.000	0.456	0.750
P9	10	2	0.000	0.000	0.000	0.000	0.028	0.039
P10	4	1	0.000	0.200	0.633	0.011	0.728	0.889
Average	–	–	0.000	0.190	0.324	0.008	0.434	0.567

50 authentication attempts by visually impaired individuals. RHYTHM TAP demonstrates high authentication accuracy with an average Area Under the Curve (AUC) of 89.7% and an average Equal Error Rate (EER) of 5.32%. Although direct comparisons are difficult because most of the related studies did not adopt the standard metrics such as AUC and EER that are commonly used in evaluating authentication technologies [2], the similar screen-tap authentication PassChords [3] showed an error rate of 16.3% and an average accuracy of 83.6% for the OneButtonPin [4]. RHYTHM TAP can achieve higher accuracy compared to prior research.

Table I presents authentication accuracies of 99.2% for visually impaired participants and 98.6% for sighted individuals within the first 5 of 50 trials. A follow-up assessment of RHYTHM TAP's accuracy was conducted one month after the initial study with 10 sighted participants, replicating the original methodology. The system achieved 99.0% accuracy within the first 5 trials and 90.5% overall accuracy over 50 trials, demonstrating robust performance over time and resistance to temporal degradation.

Table II presents the results of three different attack strategies executed by six attackers against seven target users. Attack success rates are generally lower within the first 5 attempts compared to 50 attempts, reflecting real-world security practices like account locking. Brute Force attacks are the least effective, followed by Visual Impersonation and AudioVisual Impersonation, with the latter being the most effective due to knowledge of the rhythm and music. Shorter rhythms increase attack success rates, with durations over 5 seconds recommended for better security. Using multiple smartphone surfaces for rhythm input further reduces vulnerability; for instance, participants using two surfaces and longer rhythms (e.g., 10 seconds) experienced significantly lower attack success rates, even against the more advanced AudioVisual Impersonation attacks.

The SUS scores for the visually impaired participants had a minimum of 77.5, a median of 87.5, a maximum of 100, and an average of 89 (Grade A). The standard deviation was 8.329, reflecting high user satisfaction (See Figure 3). The simple, memory-free rhythm authentication method was well-received, with participants appreciating the reduced visual strain and ease of device operation. Some also found the music-based rhythm authentication enjoyable and appealing.

IV. DISCUSSION

Fatigue and Accuracy. Extended authentication attempts during the study revealed that user fatigue may reduce accuracy. However, in typical daily scenarios with fewer authentication attempts, this effect is minimal.

Rhythm Length and Security. Longer rhythms and multiple smartphone surfaces substantially enhance resistance to impersonation attacks. Participants who used rhythms exceeding five seconds and two surfaces exhibited significantly lower attack success rates. This suggests that encouraging diversity in rhythm patterns can further strengthen security.

User Preferences. Visually impaired users valued the system's reduction in reliance on visual cues, while sighted users expressed interest in using RHYTHM TAP as a secondary authentication method in scenarios where primary methods fail, such as during groggy mornings.

Sample size. The current evaluation of RHYTHM TAP involves a relatively small sample size (n = 7) of visually impaired participants, which introduces certain limitations in generalizing our findings. This limited sample size reflects the inherent challenges in recruiting visually impaired participants for research studies.

Ethical Considerations. In conducting our user study, we carefully followed the ethical standards and regulations established by the University's IRB. Our procedures were designed to ensure full compliance with these guidelines, resulting in the confirmation of exempt status for our study.

V. CONCLUSION

RHYTHM TAP introduces a novel, inclusive approach to authentication by utilizing rhythmic tapping patterns. Its high accuracy, security, and usability make it a promising alternative to traditional methods, especially for visually impaired users. Future work will focus on expanding its application to diverse environments and enhancing resistance to advanced attack scenarios.

REFERENCES

[1] Georgia Gallavin. *System Usability Scale (SUS): Improving Products Since 1986*. https://digital.gov/2014/08/29/system-usability-scale-improving-products-since-1986/. Feb. 2022.

[2] Shridatt Sugrim et al. "Robust Performance Metrics for Authentication Systems". In: *26th Annual Network and Distributed System Security Symposium, NDSS 2019, San Diego, California, USA, February 24-27, 2019*. The Internet Society, 2019.

[3] Shiri Azenkot et al. "PassChords: secure multi-touch authentication for blind people". In: *Proceedings of the 14th International ACM SIGACCESS Conference on Computers and Accessibility*. ASSETS '12. Boulder, Colorado, USA: Association for Computing Machinery, 2012, pp. 159–166. ISBN: 9781450313216.

[4] Manisha Varma Kamarushi et al. "OneButtonPIN: A Single Button Authentication Method for Blind or Low Vision Users to Improve Accessibility and Prevent Eavesdropping". In: *Proc. ACM Hum.-Comput. Interact.* 6.MHCI (Sept. 2022). DOI: 10.1145/3546747. URL: https://doi.org/10.1145/3546747.

Poster: Rhythm Tap: Inclusive Personal Authentication Method Based on Rhythmic Variation

Yuri Takase[1], Yuto Toshikawa[1], Kazuki Nomoto[1], Ryo Iijima[1,5], Masataka Kakinouchi[2], Tatsuya Mori[1,3,4]

[1]Waseda University [2]Tsukuba University of Technology [3]NICT [4]RIKEN [5]AIST

Introduction

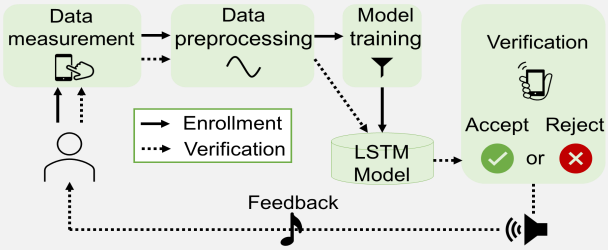
- Smartphones are essential tools for storing personal information, but traditional authentication methods (such as biometrics, passcodes, and pattern locks) pose challenges for visually impaired users.
- We propose "**RHYTHM TAP**," an inclusive authentication technology designed to enhance usability and accessibility, particularly for visually impaired users.
- This innovative method leverages **individual differences in rhythm perception**.

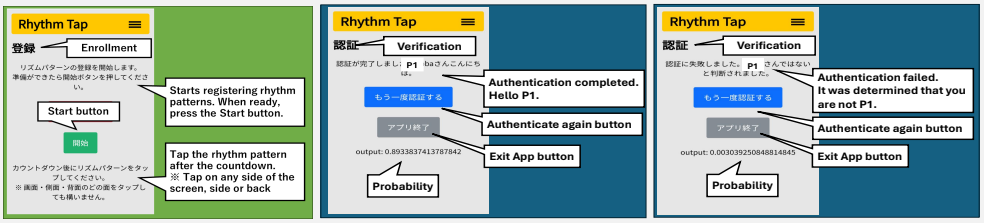
Overview of RHYTHM TAP

★ A novel authentication method leveraging individual differences in rhythm perception. Uses tapping patterns as a form of behavioral biometrics.

Enrollment Phase: Users tap rhythmically on their smartphone, and the accelerometer captures the data. The LSTM (Long Short-Term Memory) model learns the unique rhythm pattern.

Authentication Phase: Real-time tapping data is compared to the registered pattern. Results are communicated to the user, including auditory feedback.





App screen at registration. App screen upon successful /failed authentication.

Experiment Setup

Device : Android mobilephone (HUAWEI P20 lite).

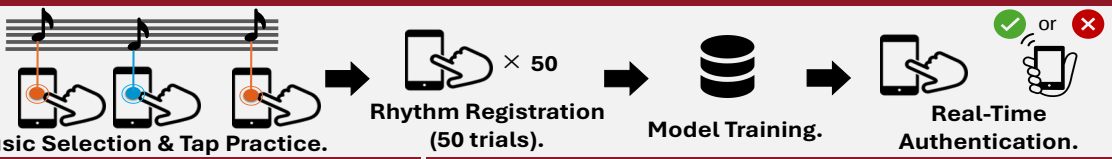
Participants: 7 visually impaired & 10 sighted individuals (19-24 years old, 11 males & 6 females).

Surfaces => S: Side, B: Back, F: Front / Screen
Visual impairment level => LB: Low vision, B: Blind

Table: CONDITIONS FOR **VISUALLY IMPAIRED & SIGTED** PARTICIPANTS.

	VISUALLY IMPAIRED							SIGHTED								
Participants	P1	P2	P3	P4	P5	P6	P7	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10
Tapping Surface	S	B,F	B,F	S	F	F	F	B	B	S,F	S,F	S	F,S	F	B	F,B	F
Rhythm Duration (s)	3	8	10	6	8	3	15	7	2	5	2	4	5	6	9	10	4
Visual impairment level	B	LB	B	LB	B	LB	LB	-	-	-	-	-	-	-	-	-	-

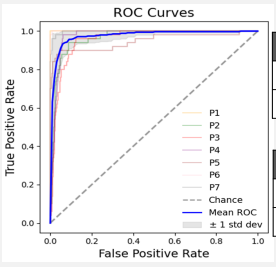
Procedures



Music Selection & Tap Practice. Rhythm Registration (50 trials). Model Training. Real-Time Authentication.

- Breaks are scheduled between tasks to reduce participant fatigue.
- Accessibility tools like TalkBack are provided for visually impaired users.

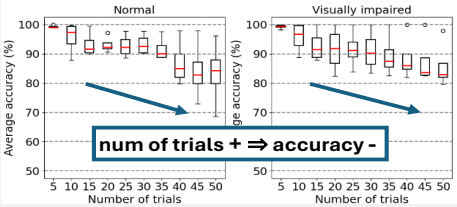
Result: *ROC Curve* (visually impaired)



	Avg. AUC
Ours	**0.897**
[1]	**0.836**

	Avg. EER
Ours	**0.0532**
[2]	**0.163**

Result: Avg. Accuracy vs Num of Trials



	First 5 trails	Total 50 trails
Visually impaired	**0.992**	0.897
Sighted	**0.986**	0.952

Result: Robustness Over Time

Evaluated again 1 month later with 10 same sighted participants.

First 5 trails	Total 50 trails
0.9900	0.9947

Result: ASR for Three Attack Scenarios

Target	T	m	$r_b(5)$	$r_v(5)$	$r_{av}(5)$	$r_b(50)$	$r_v(50)$	$r_{av}(50)$
P1	7	1	0.000	0.133	0.533	0.017	0.750	0.922
P2	2	1	0.000	1.000	1.000	0.028	0.961	1.000
P6	5	2	0.000	0.000	0.000	0.000	0.022	0.061
P9	10	2	0.000	0.000	0.000	0.000	0.028	0.039
P10	4	1	0.000	0.200	0.633	0.011	0.728	0.889
Avg.	-	-	**0.000**	**0.190**	**0.324**	**0.000**	**0.434**	**0.567**

T: Rhythm Length(s), m: Number of used surfaces, r_b: Brute Force Attacks, r_v: Visual Impersonation Attacks, r_{av}: AudioVisual Impersonation Attacks

Attack Success Rates: Lower within first 5 attempts.

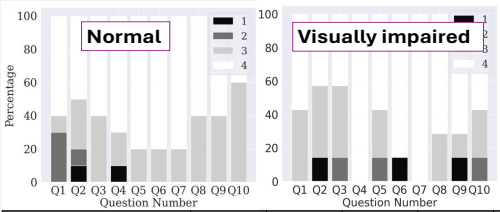
Attack Types: Brute Force < Visual Impersonation < AudioVisual Impersonation.

Shorter Rhythms: Higher vulnerability; >5 seconds.

Multiple Surfaces: Enhanced security with 2+ surfaces.

Example: 10-sec rhythm + 2 surfaces = low attack success rates.

Result: Usability Study (SUS questionnaire)



+ Positive
Simple, Accessible, Enjoyable

- Negative
Consistency, Reliability concerns

	min	mdn	max	avg	SD
Normal	77.5	91.25	97.5	**89**	7.472
Visually impaired	77.5	87.5	100	**89**	8.329

Rank A (89 > 68)

Discussion

- **Fatigue Impact:**
  - Minimal impact on daily use; accuracy drops with extended attempts.
- **User Preferences:**
  - Visually impaired: Appreciate reduced visual reliance.
  - Sighted: Favor as a backup method.
- **Sample Size:**
  - Limited (n=7 visually impaired); challenges in broader generalization.

Future Work

- **Diverse Participants:**
  - Evaluate with different ages, cultures, and abilities.
- **Real-World Scenario:**
  - Evaluate in noisy and mobile environments.

Reference

[1] Kamarushi et al.. "OneButtonPIN: A Single Button Authentication Method for Blind or LowVision Users to Improve Accessibility and Prevent Eavesdropping".

[2] Shiri Azenkot et al. "PassChords: secure multi-touch authentication for blind people".