



Is Crowdsourcing a Puppet Show? Detecting a New Type of Fraud in Online Platforms*

Shengqian Wang, Israt Jahan Jui, Julie Thorpe

MOTIVATION

Crowdsourcing platforms such as Amazon Mechanical Turk (MTurk) have emerged as popular tools for studies with human subjects.

We conducted 2 studies on Amazon MTurk and found some anomalies in our datasets, prompting us to perform the analysis presented herein.

CONTRIBUTIONS

1. We identify a new threat we call **puppeteers**, which are workers controlling multiple **puppet** accounts that appear human.
2. We quantify puppeteer fraud on MTurk, finding **34% to 55% accounts are puppets**.
3. We propose novel puppet detection methods.

METHODOLOGY

Study 1 (3 Conditions, 2 Sessions)

- Participants interacted with our system, created passwords, and answered questionnaires.

Study 2 (4 Conditions, 2 Sessions)

- Participants were assigned a random 4-digit PIN, which was placed in their browser's local storage. They interacted with our system, and answered questionnaires.

POTENTIAL DETECTION STRATEGIES

Strategies	Detect Puppets?	Detect Bots?
1. Behavioral anomaly detection	✓	✓
2. Implicit learning tasks	✓	✓
3. Dynamic questions & context	✓	✓
4. Highly unique answers	✓	✓
5. Fingerprint & local storage values	✓	✓
6. Text-to-Image conversion	✓	✓

FUTURE WORK

- Investigating puppeteer prevalence on other platforms (e.g., Prolific).
- Developing robust detection tools.
- Evaluating long-term impacts and evolving tactics.

DETECTING PUPPET ACCOUNTS

Study 1: Many participants chose the same password. To estimate how likely this repetition was by chance, we used a binomial distribution and data from a large corpus of leaked passwords dataset [1]. We estimate p using m/c , where m is the frequency (number of occurrences) of a particular password in the dataset and $c=5,579,399,834$ is the total number of unique passwords. Using this p , the probability of seeing that password at least k times among n participants is approximated by:

$$P(X \geq k) = 1 - P(X < k) = 1 - \sum_{x=0}^{k-1} \binom{n}{x} p^x (1-p)^{n-x}$$

Puppeteers	No. of Accounts (k)	Probability of Success (p)	Probability ($P(X \geq k)$)	Puppeteers	No. of Accounts (k)	Probability of Success (p)	Probability ($P(X \geq k)$)
Pup_15	3	4.12×10^{-5}	1.6×10^{-5}	Pup_9	2	2.00×10^{-10}	3.3×10^{-16}
Pup_20	5	1.69×10^{-4}	2.4×10^{-6}	Pup_11	2	2.00×10^{-10}	3.3×10^{-16}
Pup_6	2	5.75×10^{-6}	6.0×10^{-7}	Pup_12	2	2.00×10^{-10}	3.3×10^{-16}
Pup_1	2	1.50×10^{-6}	1.8×10^{-7}	Pup_13	2	2.00×10^{-10}	3.3×10^{-16}
Pup_4	2	1.81×10^{-6}	1.6×10^{-7}	Pup_28	8	4.54×10^{-6}	1.2×10^{-19}
Pup_7	2	1.30×10^{-6}	1.1×10^{-7}	Pup_14	3	2.00×10^{-10}	1.8×10^{-23}
Pup_5	2	1.15×10^{-6}	7.6×10^{-8}	Pup_16	3	2.00×10^{-10}	1.8×10^{-23}
Pup_18	4	1.35×10^{-5}	1.1×10^{-8}	Pup_30	19	1.24×10^{-3}	2.3×10^{-26}
Pup_10	2	1.20×10^{-8}	1.2×10^{-12}	Pup_22	5	3.82×10^{-8}	1.0×10^{-27}
Pup_24	7	7.40×10^{-4}	2.2×10^{-12}	Pup_25	7	1.31×10^{-6}	3.2×10^{-29}
Pup_17	4	6.84×10^{-7}	5.0×10^{-13}	Pup_19	4	2.00×10^{-10}	1.2×10^{-31}
Pup_27	8	1.99×10^{-5}	1.1×10^{-13}	Pup_23	5	8.10×10^{-9}	1.2×10^{-32}
Pup_3	2	3.20×10^{-9}	8.4×10^{-14}	Pup_26	7	1.40×10^{-9}	1.7×10^{-50}
Pup_21	5	3.22×10^{-6}	1.5×10^{-17}	Pup_29	13	2.00×10^{-10}	2.1×10^{-74}
Pup_2	2	2.00×10^{-10}	3.3×10^{-16}	Pup_31	57	3.90×10^{-9}	4.5×10^{-279}
Pup_8	2	2.00×10^{-10}	3.3×10^{-16}				

Table 3: Suspected puppeteers in Study 1.

Study 2: Our system assigned a random PIN to each participant, and placed it in their browser's local storage. We calculated the probability of seeing the same PIN twice for 2 participants in our largest group as 0.00016, so any participants with the same PIN were considered a puppet account. We identified at least 38 distinct puppeteers, each having between 2-8 puppet accounts.

RESULTS

We identified a large number of puppet accounts in both studies: Study 1 had 193 puppet accounts (34.6%), including up to 57 controlled by a single entity, and Study 2 had 394 puppet accounts (55%).

	C1	C2	C3	Overall
Participants	181	185	192	558 (100%)
Puppets	76	53	64	193 (34.6%)
Inattentive	34	49	44	127 (22.7%)
Valid Workers	71	83	84	238 (42.7%)

Table 1: Study 1 summary

	C1	C2	C3	C4	Overall
Participants	167	181	178	172	698 (100%)
Puppets	88	97	91	108	384 (55%)
Valid Workers	77	84	87	69	317 (45%)

Table 2: Study 2 summary



Figure 1: Screenshots from social media groups openly advertising MTurk accounts for sale or rent, illustrating the ease with which puppeteers can acquire multiple puppet accounts.

References: [1] Stefán Jökull Sigurðarson, PwnedPasswordsDownloader, GitHub, <https://github.com/HavelBeenPwned/PwnedPasswordsDownloader>, last accessed Mar. 24, 2025.

