Using Theme-based Narrative Construct of Images as Passwords: Implementation and Assessment of Remembered Sequences

https://doi.org/10.3991/ijoe.v13i11.7774

Priya Chellaiah, Bipin Nair, Krishnashree Achuthan, Shyam Diwakar(✉)
Amrita Vishwa Vidyapeetham (Amrita University), Amritapuri, Kollam, Kerala, India
shyam@amrita.edu

Abstract—With many online engineering platforms such as virtual and remote laboratories designed for young or aged users, user authentication and passwords-based methods are being re-evaluated for tracking usage patterns and security. For ICT-enabled online engineering platforms, image-based human-centric approaches are gaining relevance for access frameworks. With the rubber-hose attacks, increased senior users, many existing systems are vulnerable to many attacks. This paper employs human uniqueness of narrative skills on an image-based password system for online platforms with focus on theme in the password generation process. To generate the secret password, a specially designed computer game was used. We used narrative constructs composed of cartoon image sequences to generate user-specific secret key. The durability of generated passwords and the authentication process while assessing the reconstruction process by a potential hacker was verified. For validating use of coerced attacks, under imposed psychological duress, users failed retrieving the password sequence suggesting the reliability as an anti-coercive attack cybersecurity tool. A set of experiments were used to analyze user behavior behind the image-based password system. EEG measurements demonstrated increased activity of α rhythms in F3 and FC5 channel bins and augmented levels of β rhythms in F3 and O1 channels, suggesting users added personalization to authentication more than in alpha-numeric password-based logins.

Keywords—Cybersecurity, Image-based passwords, Authentication, Sequence Learning, Cartoon Sequence, ElectroEncephaloGraphy.

1 Introduction

Online platforms such as virtual laboratories and skill training have shown a wide variety of users and tracking analytical data from such platforms indicate novel learning trends and pedagogies [1], [2]. Federated e-Sciences platforms require better user interfaces with reliable tracking systems and has been perceived as key for Science 2.0. Many tracking systems rely on authentication frameworks. With aged users and young learners in ICT environments, access control methods have been adapted differently to suit usage patterns [3], [4]. Having developed over 350 freely available online laboratories (see vlab.amrita.edu), our studies on user groups suggested the need to develop unique user authentication systems for aged and very young learners who had problems with password-based authentication. With trust being key in user authentication in ICT environments, security methods employ secret keys such as alphanumeric passwords, biometric features, hardware tokens, graphical passwords etc. Stored passwords are vulnerable to eavesdropping, dictionary attacks, social engineering, and shoulder-surfing. Apart password phrases, there are many other ways to retain physical control of the device via hardware tokens, fingerprints, iris patterns, walking gait etc.[5]–[8]. Compromised biometric methods complicate authentication schemes due to inability to modifications. The primary drawback of human role in apriori knowledge-based authentication schemes is the limitation in recalling secure passwords. To overcome this problem, image sequences were used. Graphical passwords employ the cognitive ability to understand and recall images[9],[10]. Using cartoon or character sequences and graphical authentication systems including CAPTCHAs have been an alternative to knowledge-based passwords to biometric authentication[11],[12]. reCAPTCHA have been introduced as a secondary authentication technique to prevent unauthorized access from automated bots, however it is a challenge response method [13].

Humans have an innate ability to remember patterns and images rather than numbers and sequences. Health organizations have used combination of images and text [14] to improve the health communication. Studies report comic strips playing a strategic role in expanding the opportunities in teaching and learning, and have shown a decrease in social loneliness and increased satisfaction in students with autism spectrum disorder[15],[16]. An authentication system[17] based on implicit learning from cognitive psychology[18], where passwords were generated using a special task called serial interception sequence learning (SISL) was proposed as a preliminary implementation. Users were trained on a secret key of 30-character length in a 45-minute training session. Even though the learned secrets were supposed to be impossible to recall verbally or to write it down, the duration of password generation was a big limitation. To overcome this limitation, we introduced image sequences of specific length instead of character sequence, by considering the human ability to remember graphical information rather than lengthy character sequences.

Uniqueness of human cognition and perceptive distinctiveness of the brain plays a major role in user-generated passwords and this capability was employed in this study to develop passkeys based on user's personal grammar of an image sequence. In this paper, we highlight a novel technique using narrative skills towards image based authentication using the user's ability to associate cartoon strip patterns, while being unable to explain the choice behind such patterns and the failure of authentication during induced stress. This sequence arrangement was designed as a special task called Narrative Construction Sequence Learning (NCSL) and was used to train users to generate a unique passkey. The proposed system includes two phases: Training and Authentication. We are introducing the NCSL task as a semi-implicit or pseudo-implicit motor learning task, since the task requires the users actions for motor command and sensory feedback to drag and drop the selected images and may be stored in memory as components of a learning process [19]. The methodology also employs narrative cognitive training, an evaluation of individuals cognitive aspects and basic executive functions as battery tasks which can be treated as authentic identities[20]. This task can also be considered as a Serial Reaction Time (SRT) task [21] assessing the users reaction time which decreases for repeating sequence. Abilities to correlate with specific cartoon-based strips have been understood by nature of the associativity of patterns [22] stored in the memory and the learning rule highly affects the accuracy of recall. This correlation between the images and the memory construct was used to implement the system described in this paper with the focus of enabling aged and young users in online engineering platforms.

2 Narrative Construction Based Task

The Narrative Construction Sequence Learning (NCSL) task was based on the idea of sequence learning explained in[23]. In this implementation, there were four categories of sequence learning problems:

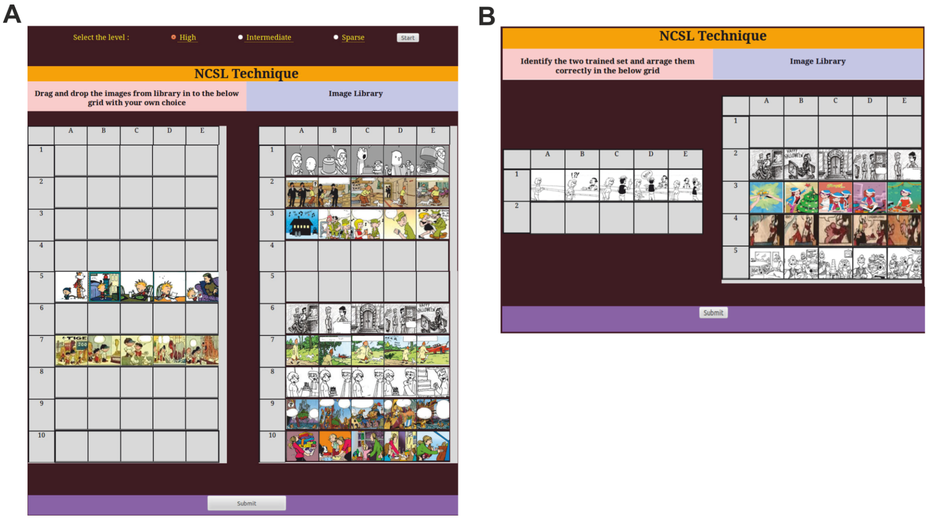
1. Sequence Prediction: The user, considering the preceding image predicted the images (elements) in the sequence.
2. Sequence generation: Specific themes defined the attempts to generate the images sequence. The images within a set had some implicit or explicit characteristics related to the specific theme.
3. Sequence Recognition: Legitimacy of the elements in the sequence were evaluated by observing the cartoon characters in the images within a set.
4. Sequential decision-making: Decision-making involved when the sequence of actions accomplished a goal. In the implemented system, the goal was successful user-authentication.

In mathematical terms, the client generates a password sequence x, composed of a themed sequence of images, $U_{i.}$ (of sequence size i) and the server is given a set of sequences $(f^{i}(x), U)$. Two key concepts used in NCSL were narration and sequence order. In NCSL task, by allowing the user to vary the length of sequences, we studied how users managed multiple themes in a process of narration. Three different modes of narration were used: easy (consisted of three cartoon images forming a sequence), medium (had five images) and difficult (had eight images). Medium mode was used for training and the other two for testing purpose. It was assumed that the order of images in a sequence acted as the critical element behind the themes. User could decide the sequence order and hence multiple orders for each sequence were possible. This helped to increase the combinations among number of secret keys and aided users to have unique passkey sequences. In NCSL task, the users developed sensitivity to the structured information by intercepting the given images. Narration was chosen to play a major role in NCSL task. Themes based on image sequences were formed using cartoon images (see Fig. 1). Each theme consisted of different sets of finite number of images to be ordered by the user. Each image, within a set, represented an event that could occur in that theme. The themes (see Table 1 for examples) were real life scenarios such as, having dinner, going for a trip, preparing food etc. An image library containing different themes was presented on the right side and an empty grid was presented on the left side of the computer screen. The sizes of the empty grid were different and were referred as levels.

Table 1. Example Themes and Events

Theme	Example events
Having Dinner	A boy playing with friends, returning home, finishing homework, have dinner, go to sleep
Going for a trip	Planning, packing the luggage, getting into the bus, enjoying the trip, camp fire
Preparing food	Planning the food item, getting the required ingredients, cleaning the ingredients, cooking food, serving food

There were three training levels such as High, Intermediate and Sparse. High security level (see Fig. 1A) was a training sequence where users had to arrange 10 sequence sets of 5 images each. Intermediate training was when a user had to arrange 4 sequences of 5 images and sparse was three sequences of 5 images each. The training goal, interception of the sequences, was performed by selecting images from same theme and arranging it in the grid provided on the left side in an order, chosen by user without any specific inputs. Training task was to make a user repeat several sets of image sequences within a specific theme (75%) more than other themes presented as the image library. During the 5 or 10-minute training process, user performed several NCSL tasks and training was a process that involved repeating themes during 75% of the trials. Participants were expected to identify the themes by repeatedly performing the NCSL task during training. The task was designed for users to perform better on the trained data at the time of authentication. All themes contained images from various cartoon strips and did not have any textual dialogues. Textual dialogues were avoided to prevent explicit arrangement of images.



Drag and drop the images from library in to the below grid with your own choice

Identify the two trained set and arrage them correctly in the below grid

Fig. 1. Screenshots of training and authentication tasks in progress.

The goal of training was that the user performed better on the trained themes and did not consciously recall the order of the images in the theme. Users were presented with the NCSL task through an application via web browser and were processed via a login form. Participants could perform NCSL task, data from which was logged on completion of training.

User Behavior Assessment. As a preliminary assessment[24], to evaluate user brain activity behavior behind the proposed system, EEG data was collected from 4 healthy volunteers of mean age 23 after an informed consent and prior ethical clearance from institutional committee. A commercial EEG headset [25] with14+2 channel electrodes was employed and experiments were conducted in a noise free environment. For this study, we used NCSL task and recordings were done in three modes: relaxation, training and authentication. In relaxed mode, subjects were asked to focus in to a blank screen and relax for 2 minutes and the brain wave signals were recorded. For the other two modes, NCSL training and authentication tasks were used. 3 trials for each subject were recorded for each task. The maximum time taken to record each task was an average of 5 minutes. After recording EEG signals during each mode, raw traces were processed to remove artifacts using a bandpass filter. To quantify user-level variations, we considered only (7.5 - 12.5) and (12.5 - 30) waves and removed the other frequencies. After filtering, the obtained data was frequency transformed using Fast Fourier Transform (FFT) and the power spectrum was calculated using EEGLAB [26].

3 Implementation of Training and Authentication Mechanisms

NCSL was designed in two phases as training followed by authentication. NCSL training levels (high, intermediate and sparse) were used by participants to choose their own different levels of narration and to analyze the amount of sequence learning happening in users with different learning capacity.

3.1 Training

Training phase is the passkey generation phase. The training procedure involved:

Displaying an image library (See Fig. 1A) consisting of five different themes each with at least two sets selected randomly from the input data on the right side of the screen.

- Depending on choice of training level, a grid of specific size would be displayed on the left side of the screen.
- Perform the NCSL task by choosing the images from the image library and arrange it in the grid based on their discretion.
- Repeat the NCSL task for the remaining sets then submit the training. During training, 50 (from 10 sets) images were presented to the user and the duration of training depended on the training levels. The average training time was 5-10 minutes

for users to arrange sets of sequences. The system recorded the final order of the images for later use.

3.2 Authentication

During authentication (see Fig. 1B), the trained user was presented with the NCSL task, where the image library contained sets from trained and untrained themes. The authentication procedure involved:

- Presenting an image library consists of five random sets, two trained sets and three untrained sets on right side and an empty grid of size 2x5 on left side.
- The NCSL task was performed by identifying two of the trained sets and arranging the images in the selected sets in the same order as they did during training.

A trained user could identify the sets from remembered image sequences during training. The user validated identity by exhibiting better performance on the trained sets than untrained sets. When the user identified both trained sets correctly and by arranging in correct order, the system then notified authentication success.

3.3 Feedback collection

Six questions were included in the user feedback, post-training (see Table 2). Five questions were posed to each participant to rate their performance after authentication (see Table 3). Internal consistency was checked using Cronbach's alpha value.

Table 2. Feedback on Training Data

Question	Answer			
How did you choose the first image?	Random	Based on interest	Based on logical thinking	Events in daily life
	12.5%	33.3%	50%	33.3%
How did you choose the rest of the images?	Based on previous Image	Random	Based on idea	Events in daily life
	43.7%	0%	43.7%	12.5%
Which was the order of preference to arrange the images?	Left-to-right	Right-to-left	Random	
	100%	0%	0%	
How did you choose the sets from library?	Random	Based on some events	Based on interest	Easily memorable images
	33.3%	33.3%	25%	37.5%
How many sets could you remember?	1	2 to 4	5 to 6	All
	12.5%	6.25%	56.25%	25%
Are you able to remember the sequence of images in each set?	Yes	No	Some of them	
	62.5%	0%	37.5	

Online performance was correlated to learning behaviour via a feedback post-training sessions.

Table 3. Measure of Sequence Learning

Question	Answer		
How many sets could you identify?	Two	One	None
	100%	0%	0%
How did you identify the sets?	By memory	Guess work	
	93.75	6.25%	
How many sets were arranged correctly?	Two	One	
	87.5	12.5%	
Out of total images in a set, how many of them could be sequenced correctly?	Five	Four	Three
	87.5%	6.25%	6.25%
Do you remember the reason for arranging the set?	Yes	No	I don't know
	93.75%	6.25%	0%

User feedback on authentication, correlated as sequence learning rate of the user.

4 Results: User-Usability Experiments

The feasibility and usability of NCSL tool was tested with the help of volunteering participants and via direct feedback collection. We emulated an attacker by asking users to describe the narration to volunteer attacker who tried authentication but the attacker could not repeat the narrative performance as that of authenticated user (data not shown). In the following tests, NCSL tasks reliability with user's age was evaluated. Secondly, we verified that the users could retain the learned secrets for one or two weeks. The role of psychological duress on the sequences learned was also assessed. Additionally, the error rate during training and authentication for user under external influence was also estimated. Consistency among the user responses was used to estimate that the user's ability to resolve the effectiveness of the sequence is undermining compared to the ordination of the sequence.

4.1 Experiment 1: Evaluation of sequence Learning and User Age

The goal was to test whether sequence learning was independent of age of the user. Subject group included 30 participants of ages between 21 and 70. The experiment used the training procedure, where the training phase contained 50 trials and took 5-10 minutes to complete. After the training session, participants completed the authentication test that estimated learning of each participant. In this immediate test, participants successfully identified two trained sets and performed NCSL task (see Fig. 2A for successful authentication and error rate in authentication for each age group). The percentage of successful authentication is higher than the error rate which suggests sequence learning was partially dependent on age (Fig. 3A). After completing the NCSL tasks, a feedback on recalling trained sets was collected. 80 % of user's identified trained themes (Fig. 2B). The number of inputs for which the user could recall explicitly was very large and the embedded secret was a precise sequence set. An attack required the adversary to reconstruct the sequence, which was not easy without

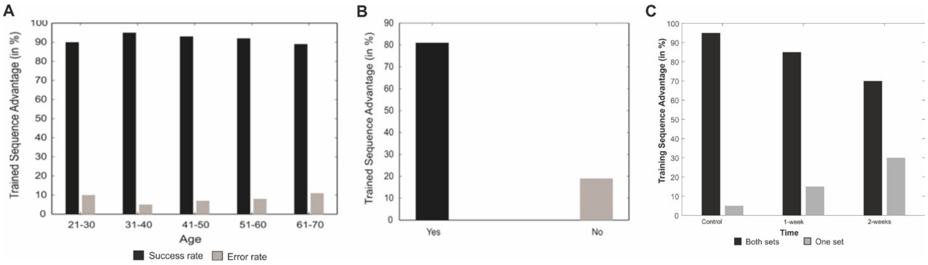


Fig. 2. Sequence Learning in NCSL. A. Instantaneous learning was counted as explicit learning as the user had immediate feedback on trained sequences. B. Theme identification for NCSL task. Yes shows the percentage of participants who identified the correct theme. No denotes the percentage of participants who identified the themes not authenticated. C.Delay and authentication. As the delay in the number of weeks post-training increased, success rate decreased.

embedding the same sequence predicate resembling users selection during training. A hypothetical attacker would have the probability of $6.4470*10^{25}$ combinations for brute-force reassembly of narrative image sequences.

4.2 Experiment 2: Recall over Time

The objective of the second set of experiments was to understand whether long breaks or time delays changed recall of the identified pattern. In a first session, participants completed the training session as they had done in experiment 1. The control group performed the NCSL authentication immediately after training to assess sequence knowledge before the delay. A group of 20 participants performed the retention and recognition assessment for the trained sequence after a week's delay. Another group of 30 participants performed the recall test after a delay of 2 weeks (see Fig. 2C). 95% of the participants in the control group identified both sets and arranged them correctly and 5% of them failed to arrange the sets. 90% of participants in the 1-week group identified both trained sets and authenticated successfully by performing the NCSL task. 10% of the participant's identified both trained sets but failed in arranging one set.70% of the participants in 2-week group identified both trained set but failed in arranging one set. 30% of the participants identified both trained sets but failed in arranging both the sets. In the tests, the participants could not recall the order of sequences after a longer delay beyond two weeks.

4.3 Error Analysis

Error rate was estimate as the sum of failures in arranging the sequences when authentication was performed. To estimate error, the NCSL experiments were performed with delay after training; varying participant age and training time (see Fig.3).

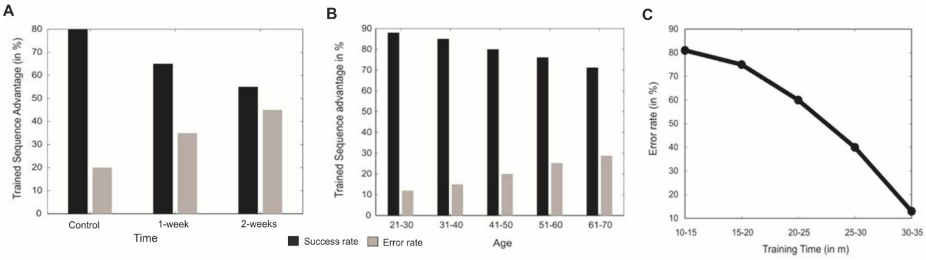


Fig. 3. Authentication error rate. A. Error rate increased with time as the participants perform training based on control. B. Error rate increased upon age when the participants perform training based on control rather than their discretion. C. Error rate gradually decreased upon increase in training time.

To evaluate whether the choice in arranging the sequence affected the learning, 10 participants were requested to train per a pre-determined order rather than employing their own choice. All participants could successfully complete the authentication test (see Fig. 3A). The group performed the authentication test a week later and a 33% error rate was observed. After two weeks, the error rate increased to 47%. Users who performed training per their discretion were able to retain the correct order of the sequence after a week and noticed that there existed a small error percentage. Error rate increased with age (Fig. 3B). The role of training time on users was studied and the average training time for reasonable success was 30 to 35 minutes, with high security level. It was observed that the error rate and training time were inversely relative (see Fig. 3C) with respect to the NCSL tasks.

4.4 Authentication Failure Under Psychological Duress

Since implementing an image-based password that relies on individual user behavior was the goal, we tested the role of imposed stress on the nature of recall of trained patterns. Experiment involved 30 participants from different age groups. Participants were put under duress by reducing training time and asked to complete the training in time. As training time was reduced, subjects showed reduced attention (data not shown, EEG assessment is ongoing work in progress). In addition, participants were asked to play a simple puzzle game soon after the training task and before the authentication to force duress on the user. Thirty percent of the participants authenticated successfully, 16.6% of them failed in arranging the sets, 50% of them identified two trained sets but failed in arranging a single set and 3.3% of them even failed in identifying the trained sets and failed in arranging the sets (see Fig. 4A). The same group of participants performed an NCSL authentication task after a week which resulted that, all participants failed in successful authentication (see Fig. 4B). 6.6% of the participants identified both sets but failed in arranging the sets, 43.4% of them identified two sets but failed in arranging both the sets, 10% of them identified a set and failed in arranging the set. Overall, with delay between training and authentication and with imposed psychological duress, 40% of them failed in both identifying and arranging the sets.

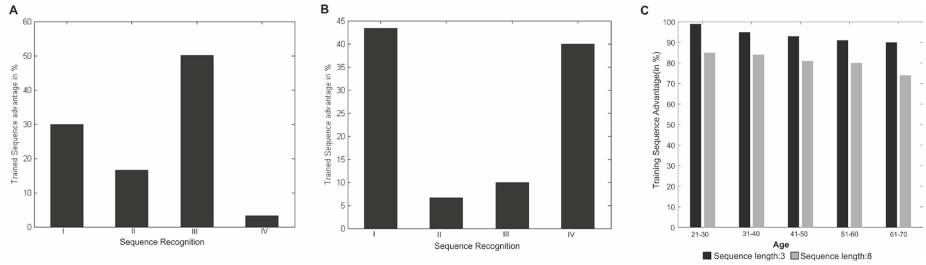


Fig. 4. Learning and recall under stress. A. Training under stress followed by authentication. I Users identified both trained sets and arranged correctly, II Users identified both trained sets but failed in arranging the sets, III Users identified both trained sets but failed in arranging one set, IV Users identified one set and failed in arranging the sets. B. Training under duress and authentication after a delay of a week showed maximum error in authentication. I-Users identified both trained sets but failed in arranging the sets, II-Users identified both trained sets but failed in arranging one set, III-Users identified one set and failed in arranging the set, IV- Users failed to identify the sets. C. Effect of sequence length on sequence learning. Short sequence resulted in explicit learning of themes whereas participants who used long sequences showed successful sequence learning through repeated training.

4.5 Sequence Length and Sequence Learning on User Training

Role of length of cartoon sequence affecting sequence learning was also evaluated. Participants could modify sequence length between 3 and 8 images per sequence. Strips with 3 images were authenticated and users could verbally express the narration. Users indicated that longer sequences were more difficult to remember (see Fig. 4C) and very difficult to express verbally (data not shown). Repeated training may enhance user's ability to verbally reconstruct some of the narration. However, longer image sequence length seemed to add efficacy to sequence learning.

4.6 Machine Learning-based Evaluation of Uniqueness in Theme

To evaluate the uniqueness present in the selected themes, we performed an image clustering. The analysis was done in two phases: clustering of uniform theme and clustering of mixed theme. We generated a dataset for uniform theme by choosing two different themes with correct set of events and performed clustering. Different clustering algorithms such as K-means, Filtered cluster, Farthest First and Make density based clusterer were used. We observed that, Make density based clusterer grouped the images with 49% in one cluster and 51% of images in other cluster, k-means grouped 45% of images in one cluster and 55% of images in other cluster, Farthest first and Filtered clusterer grouped 62%, 37% in one group and 38%, 63% in other group respectively. Images within a single theme were similar and provided uniqueness between themes. For mixed theme validation, we generated the dataset by mixing the images from different themes. Total 10 images were chosen and performed the clustering using the same set of above specified algorithms. In this case, every algorithm grouped the images in two clusters but the percental difference of the clustering was very large. 80 to 90% of the images were grouped into one cluster and the remaining were in the other cluster (see Table 4).

Table 4. Evaluation of Uniqueness in the Themes

Correct Theme				
Clustered instances (%)	***Kmeans***	***Make Density Based Clusterer***	***Filtered Clusterer***	***Farthest First***
Cluster 1	45	49	37	62
Cluster2	55	51	63	38
Incorrect Theme				
Cluster 1	82	45	82	96
Cluster2	18	55	18	4

4.7 Evaluation on Narration - Verbal Description of the Sequences Causes High Failure Rate

To evaluate the role of narration in password generation phase, an experiment with 25 users of age group between 23 and 35 was conducted. NCSL task explained in the method section was used for this experiment. Multiple sequences (one at a time) were used for this study. After completing the task, we asked them to describe the story verbally also. It was found that, for a sequence, which contains a clear theme, 60% of the users were narrated the theme uniquely even the verbal description was entirely distinct (See Fig.5.A). In case of the sequence with less distinct events, 95% of the users narrated it in alternate descriptions (See Fig.5.B).The security of the system was tested by asking some subjects to generate the passphrase with the verbal description of the story by other users and it was found that 65% of them failed to authenticate.

4.8 Cognitive Assessment

From the spectral maps plotted using the recorded EEG data, two kinds of NCSL tasks (training and authentication) and relaxed condition were analyzed for spectral activities in the regions of all 14 channels within the frequency range of α and β rhythms(see Fig.6).

In the training task, spectral activity (β) was observed at 18Hz in the occipital region represents the attention level and decision making task, and for the authentication task we observed augmented β activity at 14 and 20Hz in the occipital region. The augmented α activity was also observed in the relaxed condition at 10Hz. We compared the spectral activity of text based sign-up and sign-in processes to the image based training and authentication (see Fig.7). Using one-way ANOVA, F3 and FC5 channels show significant increase in α rhythms than the other channels (see Fig. 7A,C) both in training and authentication, where as F3 and O1 channels have shown significant β activity increase in NCSL training and authentication when compared against alphanumeric passwords (see Fig. 7B,D).

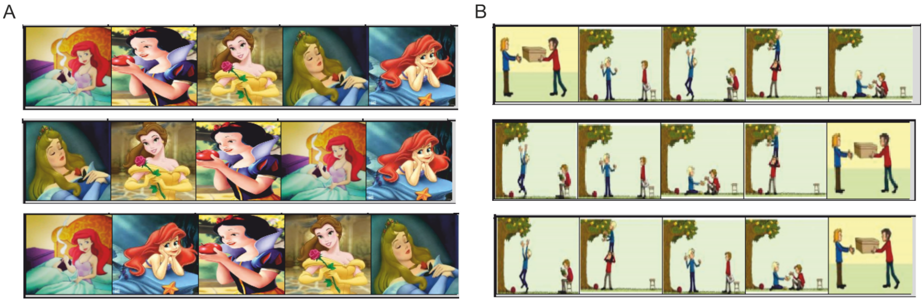


Fig. 5. Evaluation on narrative skill. A-Various possibilities in sequence narration of a single theme (which contains similar events) by multiple users. B- Various possibilities in narration of a single theme (which contains entirely different events) by multiple users.

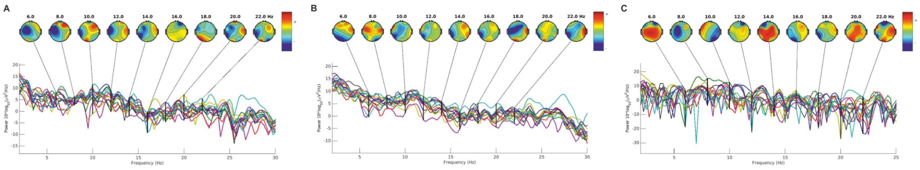


Fig. 6. EEG channel spectrum for NCSL task. A. Relaxed mode, B. Training, C. Authentication mode recordings of spectra.

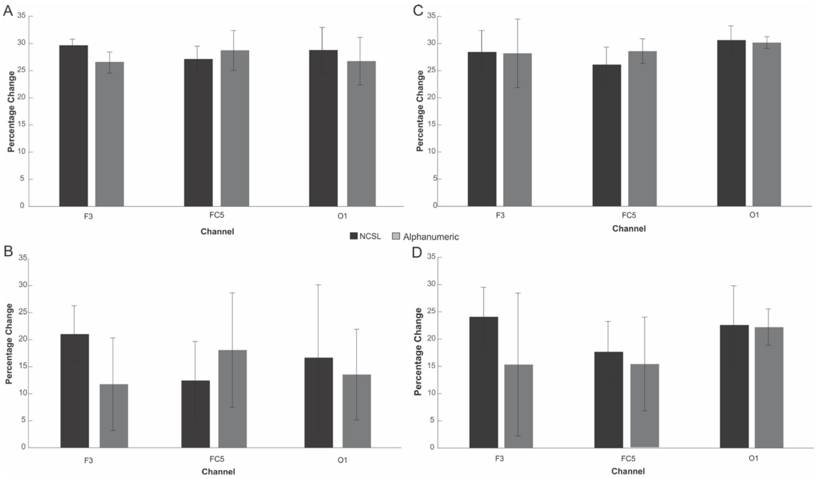


Fig. 7. Comparison on user behavior based on EEG recordings during image-based (NCSL) password and alpha-numeric password schema (3 subjects). A. Variation in α rhythm for NCSL training and alphanumeric signup task. B. Variation in β rhythm for NCSL training and alphanumeric signup task. C. Variation in α rhythm for NCSL authentication and alphanumeric sign in task. D. Variation in β rhythm for NCSL authentication and alphanumeric sign in task. A and C shows no significant change in levels of α rhythms in F3 and FC5 channels. B and D shows augmented levels of β activity in the F3 and O1 channels for NCSL, and there were no signs of increase in quantity of β rhythms in alphanumeric sign-up and sign-in when compared with NCSL.

5 Implementation Issues and Securing NCSL Code

As suggestions to secure implementation, we used file name and path name obfuscations to prevent hack attacks[27]. In a preliminary version of our code, the hacker could employ file-name and file-path to access the sequence strips and then based on a simple routine to try the permutations. Variable names and function names were obfuscated to alphanumeric random string sequences to prevent automated dictionary attacks on sequences. File path information was modified to point random location names per every session. For a man in-the-middle attack, conditional probability of both sequence and narration being guessed was computed as 1.78*1032, which implies the necessity of high computational cost and a sufficiently large combination of image sets to crack the pass sequence via a brute strategy.

6 Discussion

Using a narration-based construct arising from sequence learning, we have implemented an image-based password system appropriate for online engineering platforms such as virtual labs[28], [29], mobile banking[30] considering safer aged and children usage of ICT tools[31].

Experiments and studies on NCSL indicated that success rate for training, authentication remained significantly unchanged among various age groups, and users could learn the themes by performing the NCSL task repeatedly making NCSL applicable across ages and populations. The recall test showed that the participants failed to recall the learned secret when not used for more than two weeks suggesting infrequent usages allowed a decrease in success rate in authentication. This will have implications on applications applied to internet banking and others where it may be crucial to validate human usage and prevent machine automated accesses.

User choice in assembling patterns while training, enabled retaining passwords with lesser authentication errors, as indicated by experiments on error analysis. Results suggest that users had an advantage when not coerced into training for a known pattern. Error rate also depended on participant's age. Higher performance was consistent with younger age groups and was less consistent as age increased. In addition, longer training enforced better performance success. Although not presented in this version, the correlation between training time and age could be modified as a metric to modulate performance as a function of users learning rate.

Imposed psychological duress caused a significant change in user's success rate in authentication. Results indicate most participants failed in successful authentication under stress. While being useful, for effective authentication protocols, experiments suggest that the strength of authentication secret key was enhanced by increasing the sequence length. This failure rate under duress may help NCSL as secondary access control or login verification to deflect rubber-hose attacks.

Although electroencephalography studies are preliminary and have been posed as a pilot study to evaluate cognitive load on users for both types of logins, the data from EEG indicated in frontal lobes β rhythms were higher for NCSL tasks and showed a large variability suggesting image based passwords may involve user attention and cognitive thinking more than alphanumeric sequences. Motor task driven implicit learning models have behavior-related uniqueness and hence users rearranging of sequences was employed as an authentication process. User tests on narration showed that, uniqueness of the user to generate different versions of the same story was possible allowing several unique signatures for individual users. User behavior behind these kind of authentication systems was evaluated as pilot study with EEG, and the increase in activity may be suggestive that users added personalization to authentication more than in alpha-numeric password-based logins. Given our experiments on narration uniqueness, users attribution to generating different versions of the same story could be helpful to model authentication systems, where narration can be used as the main method to generate the password so that to ensure more security.

The time taken for the training process was longer than most traditional password-based systems but having a sequence connected via a narrative construct helped generate novel passwords that could strengthen sign-in security. On e-learning, ICT environments, banking and trust related communication and online engineering platforms, this tool can serve as a secondary layer of protection in security systems where human user authentication remains a priority.

7 Conclusion and Future Work

As a proof of concept for tracking systems and authentication frameworks for diverse online platforms, the role of narrative constructs was employed using a sequence of cartoon images to generate an image-based password system. Although, we targeted NCSL as a secondary access control mechanism due to lack of large-scale testing scenarios, a primary login replacement could be considered using a combination with social media-like phenomena to improve on a user-driven database for private image library. We are yet to implement this access authentication method on our virtual labs project (vlab.amrita.edu) which has 280000 registered users. Our future work will also aim to focus on enhancing neuroscience-based user validation as primitives towards authentication.

8 Acknowledgment

This project derives direction and ideas from the Chancellor of Amrita University, Sri Mata Amritanandamayi Devi. This work is partially supported by Virtual Labs project, NMEICT, MHRD and by Sir Visvesvaraya Faculty Fellowship to SD by MeitY, Government of India and by Embracing the World. Authors are grateful to Ross Anderson of CS Lab, Cambridge University (UK) for the inspirational role and for his suggestions on the evaluation of the NCSL technique and to Sandeep Bodda of Amrita University for EEG recordings and analysis. Authors also thank all volunteering participants who helped evaluate the technique using their feedback.

9 References

[1] S. Diwakar, D. Kumar, R. R. Radhamani, H. Sasidharakurup, N. Nizar, K. Achuthan, P. Nedungadi, R. Raman, and B. Nair, "Complementing Education via Virtual Labs: Implementation and Deployment of Remote Laboratories and Usage Analysis in South Indian Villages," *Int. J. Online Eng.*, vol. 12, no. 3, pp. 8–15, 2016. https://doi.org/10.3991/ijoe.v12i03.5391

[2] N. Tselios, N. Avouris, and V. Komis, "The effective combination of hybrid usability methods in evaluating educational applications of ICT : Issues and challenges," pp. 55–76, 2008.

[3] S. Bocconi, S. Dini, L. Ferlino, C. Martinoli, and M. Ott, "ICT Educational Tools and Visually Impaired Students: Different Answers to Different Accessibility Needs," *Univers. Access Human-Computer Interact. Appl. Serv.*, pp. 491–500, 2007.

[4] S. Sayago and J. Blat, "Older people and ICT: Towards understanding real-life usability and experiences created in everyday interactions with interactive technologies," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2009, vol. 5614 LNCS, no. PART 1, pp. 154–163.

[5] L. O'Gorman, "Comparing passwords, tokens, and biometrics for user authentication," *Proc. IEEE*, vol. 91, no. 12, pp. 2021–2040, 2003. https://doi.org/10.1109/JPROC.2003.819611

[6] A. Kale, A. Sundaresan, a. N. Rajagopalan, N. P. Cuntoor, A. K. Roy-Chowdhury, V. Krüger, and R. Chellappa, "Identification of humans using gait," *IEEE Trans. Image Process.*, vol. 13, no. 9, pp. 1163–1173, 2004. https://doi.org/10.1109/TIP.2004.832865

[7] M. Hari Priya and N. Lalithamani, "A Survey for Securing Online Payment Transaction Using Biometrics Authentication," vol. 517, Springer Verlag, 2017, pp. 81–91. https://doi.org/10.1007/978-981-10-3174-8_8

[8] A. Ashok, P. Poornachandran, and K. Achuthan, "Secure Authentication in Multimodal Biometric Systems Using Cryptographic Hash Functions," Springer, Berlin, Heidelberg, 2012, pp. 168–177. https://doi.org/10.1007/978-3-642-34135-9_17

[9] A. De Angeli, L. Coventry, G. Johnson, and K. Renaud, "Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems," *Int. J. Hum. Comput. Stud.*, vol. 63, no. 1–2, pp. 128–152, 2005. https://doi.org/10.1016/j.ijhcs.2005.04.020

[10] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: Basic Results," *Proc. 11th Human-Computer Interact. Int. Conf. (HCII 2005)*, 2005. https://doi.org/10.1145/1073001.1073002

[11] L. Wang, X. Chang, Z. Ren, H. Gao, X. Liu, and U. Aickelin, "Against spyware using CAPTCHA in graphical password scheme," *Proc. - Int. Conf. Adv. Inf. Netw. Appl. AINA*, pp. 760–767, 2010.

[12] S. S. Banne and K. N. Shedge, "CARP: CAPTCHA as A Graphical Password Based Authentication Scheme," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 5, no. 1, 2016.

[13] S. Vikram, Y. Fan, and G. Gu, "SEMAGE: a new image based two factor CAPTCHA," in *Proceedings of the 27th Annual Computer Security Applications Conference on - ACSAC '11*, 2011, pp. 237–246. https://doi.org/10.1145/2076732.2076766

[14] P. S. Houts, C. C. Doak, L. G. Doak, and M. J. Loscalzo, "The role of pictures in improving health communication: A review of research on attention, comprehension, recall, and adherence," *Patient Educ. Couns.*, vol. 61, pp. 173–190, 2006. https://doi.org/10.1016/j.pec.2005.05.004

[15] F. Megawati and M. Anugerahwati, "Comic Strips : a Study on the Teaching of Writing Narrative Texts To Indonesian Efl Students," *Teflin J.*, vol. 23, no. 2, p. 183, 2012.

[16] M. R. Pierson and B. C. Glaeser, "Using Comic Strip Conversations to Increase Social Satisfaction and Decrease Loneliness in Students with Autism Spectrum Disorder," vol. 42, no. December, pp. 460–466, 2007.

[17] S. Diwakar, P. Chellaiah, B. Nair, and K. Achuthan, "Theme Interception Sequence Learning : Deflecting Rubber-Hose Attacks Using Implicit Learning," in *Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014*, 2015, vol. 1, pp. 495–502.

[18] H. Bojinov, D. Sanchez, P. Reber, D. Boneh, and P. Lincoln, "Neuroscience Meets Cryptography : Designing Crypto Primitives Secure Against Rubber Hose Attacks," in *Proceedings of the 21st USENIX conference on Security symposium*, 2012, pp. 1–13.

[19] J. a. Adams, "Historical review and appraisal of research on the learning, retention, and transfer of human motor skills.," *Psychol. Bull.*, vol. 101, no. 1, pp. 41–74, 1987. https://doi.org/10.1037/0033-2909.101.1.41

[20] J. A. Singer, P. Blagov, M. Berry, and K. M. Oost, "Self-Defining Memories, Scripts, and the Life Story: Narrative Identity in Personality and Psychotherapy," *J. Pers.*, vol. 81, no. 6, pp. 569–582, 2013. https://doi.org/10.1111/jopy.12005

[21] M. J. Nissen and P. Bullemer, "Attention Requirements of Learning: Evidence from Performance Measures," *Cogn. Psychol.*, vol. 19, no. 1, pp. 1–32, 1987. https://doi.org/10.1016/0010-0285(87)90002-8

[22] K. V. Arya, V. Singh, P. Mitra, and P. Gupta, "Face recognition using Parallel Associative Memory," *2008 IEEE Int. Conf. Syst. Man Cybern.*, pp. 1332–1336, Oct. 2008. https://doi.org/10.1109/ICSMC.2008.4811470

[23] R. Sun and C. L. Giles, "Sequence Learning : From Recognition and Prediction to Sequential Decision Making," *IEEE Intell. Syst.*, vol. 16, pp. 67–70, 2001. https://doi.org/10.1109/MIS.2001.1463065

[24] P. Chellaiah, S. Bodda, R. Lal, C. Madhu, V. Zamarae, K. Achuthan, B. Nair, and S. Diwakar, "EEG-Based Assessment of Image Sequence-Based User Authentication in Computer Network Security," in *Proceedings of ICEEOT 2016*, 2016, pp. 3674–3677. https://doi.org/10.1109/ICEEOT.2016.7755395

[25] EMOTIV, "Emotiv Epoc and Testbench Specifications," *Brain Comput. Interface Sci. Context. EEG*, pp. 1–7, 2014.

[26] A. Delorme and S. Makeig, "EEGLAB: an open source toolbox for analysis of single-trial EEG dynamics including independent component analysis.," *J. Neurosci. Methods*, vol. 134, no. 1, pp. 9–21, Mar. 2004. https://doi.org/10.1016/j.jneumeth.2003.10.009

[27] M. Dalla Preda and R. Giacobazzi, "Semantics-based code obfuscation by abstract interpretation," *J. Comput. Secur.*, vol. 17, pp. 855–908, 2009. https://doi.org/10.3233/JCS-2009-0345

[28] S. Diwakar, H. Parasuram, C. Medini, R. Raman, P. Nedungadi, E. Wiertelak, S. Srivastava, K. Achuthan, and B. Nair, "Complementing Neurophysiology Education for Developing Countries via Cost-Effective Virtual Labs: Case Studies and Classroom Scenarios.," *J. Undergrad. Neurosci. Educ.*, vol. 12, no. 2, pp. A130-9, Jan. 2014.

[29] S. Diwakar, D. Kumar, R. Radhamani, H. Sasidharakurup, N. Nizar, K. Achuthan, P. Nedungadi, R. Raman, and B. Nair, "Complementing education via virtual labs: Implementation and deployment of remote laboratories and usage analysis in south indian villages," *Int. J. Online Eng.*, vol. 12, no. 3, pp. 8–15, 2016. https://doi.org/10.3991/ijoe.v12i03.5391

[30] A. A. Aliyu, R. Bin, and H. Tasmin, “The Impact of Information and Communication Technology on Banks " Performance and Customer Service Delivery in the Banking Industry,” *Int. J Latest Trends Fin. Eco. Sc*, vol. 2, no. 1, pp. 80–90, 2012.

[31] T. Byron, “Safer Children in a Digital World The Report of the Byron Review,” *Safer Child. a Digit. World Rep. Byron Rev.*, p. 224, 2008.

10 Authors

Priya Chellaiah is currently a Research Assistant at Amrita School of Biotechnology, Amrita University, India.

Krishnashree Achuthan is Dean, Post Graduate programs and Director, Amrita Center for Cyber-Security Systems and Networks. (e-mail: krishna@amrita.edu).

Bipin Nair is the Professor and Dean of School of Biotechnology, Amrita Vishwa Vidyapeetham University, India. (e-mail: bipin@amrita.edu).

Shyam Diwakar is Associate Professor and Lab Director of Computational Neuroscience Laboratory at the School of Biotechnology. Amrita University, India. He is a Young Faculty Fellow under Sir Visvesvaraya PhD scheme by Media Labs Asia, Ministry of Electronics and IT, Government of India. He is a Co-investigator of VALUE (Virtual and Accessible Laboratories for Universalizing Education); a virtual labs initiative supported by Sakshat mission of MHRD, Government of India, and Principle Investigator of few other projects funded by Department of Science and Technology, Government of India. (e-mail: shyam@amrita.edu).

Article submitted 28 September 2017. Published as resubmitted by the authors 30 October 2017.