



# A novel approach for designing authentication system using a picture based P300 speller

Nikhil Rathi<sup>1</sup> · Rajesh Singla<sup>1</sup> · Sheela Tiwari<sup>1</sup>

Received: 12 May 2020 / Revised: 30 September 2020 / Accepted: 8 January 2021 / Published online: 30 January 2021  
© The Author(s), under exclusive licence to Springer Nature B.V. part of Springer Nature 2021

## Abstract

Due to great advances in the field of information technology, the need for a more reliable authentication system has been growing rapidly for protecting the individual or organizational assets from online frauds. In the past, many authentication techniques have been proposed like password and tokens but these techniques suffer from many shortcomings such as offline attacks (guessing) and theft. To overcome these shortcomings, in this paper brain signal based authentication system is proposed. A Brain–Computer Interface (BCI) is a tool that provides direct human–computer interaction by analyzing brain signals. In this study, a person authentication approach that can effectively recognize users by generating unique brain signal features in response to pictures of different objects is presented. This study focuses on a P300 BCI for authentication system design. Also, three classifiers were tested: Quadratic Discriminant Analysis (QDA), K-Nearest Neighbor, and Quadratic Support Vector Machine. The results showed that the proposed visual stimuli with pictures as selection attributes obtained significantly higher classification accuracies (97%) and information transfer rates (37.14 bits/min) as compared to the conventional paradigm. The best performance was observed with the QDA as compare to other classifiers. This method is advantageous for developing brain signal based authentication application as it cannot be forged (like Shoulder surfing) and can still be used for disabled users with a brain in good running condition. The results show that reduced matrix size and modified visual stimulus typically affects the accuracy and communication speed of P300 BCI performance.

**Keywords** Brain–computer interface · P300 · Authentication · Quadratic discriminant analysis · Information transfer rate

## Introduction

With the advancement of technology, fraud cases have also been increased, therefore, security becomes the primary concern in any field, whether it is public security, personal access to a device, transactions through net banking, and e-commerce, etc. As the majority of work is to be done by the integration of modern technologies, people require a reliable, fast, and appropriate security system to protect

their assets (personal information). Therefore, authentication plays a vital role in the security of any system. Authentication is a process of detecting reported user identity by verifying the evidence presented by the user (Bhattacharyya et al. 2009). Evidence received by the user during the authentication process is called a credential. Initially, the user needs to enrol in the authentication system by creating a unique ID and password. The created entry is registered in the database as a template that is internally attached to a user ID. To gain access, users must provide the ID and password generated earlier to validate their identity. The provided information is compared to the templates stored in the database. Once the scanning is over, the system responds with approval (match) or rejection (no match). An authentication process can be described in two steps: identification and verification (Raju and Udayashankara 2018). The identification process determines the identity of an individual (El Saddik et al. 2007). During

✉ Nikhil Rathi  
nikhilr.ic.16@nitj.ac.in

Rajesh Singla  
singlar@nitj.ac.in

Sheela Tiwari  
tiwaris@nitj.ac.in

<sup>1</sup> ICE Department, Dr. B. R. Ambedkar NIT Jalandhar, GT Road Bye-Pass, Jalandhar, Punjab 144011, India

identification, credentials provided by the user are compared with several stored templates in a database. Identification systems are often described as a 1-to- $n$  matching scheme, where  $n$  is the total number of templates in the database. In the verification process, the user's credential is verified with his template stored in the database. To find a match, the system compares the requesting person's credentials against the template that already exists in the database linked to that person's account. In the verification process, 1-to-1 matching is performed as the system aims to match the individual's templates against a similar template in the database (Schomaker 2007).

Authenticating a user with a login ID and password is generally considered the most fundamental type of authentication, which relies only on the two attributes (ID and password) therefore this type of authentication is considered as single-factor authentication. An authentication factor represents a piece of information or attribute that can be used to authenticate a user seeking access to a system. Authentication factors that are commonly used include the knowledge factor (password-based), the possession factor (token-based), and the inherence factor (biometric-based) (Kwong et al. 1992). Knowledge-based methods rely on the ability of a human being to memorize i.e., something the user already knows to logins such as a password, username, and answer to a secret security question, etc. The most common example of this approach is a password-based authentication. Passwords are often used to protect personal details, such as social media accounts, internet banking, e-commerce websites, and other online platforms. This authentication technique has many limitations; particularly passwords are usually very predictable. Most individuals choose a simple combination of alphabets, digits, and symbols instead of generating complex passwords since it is easier to memorize or recall. The password-based systems are not secure and suffer from several attacks such as off-line dictionary attacks, brute force attacks, and shoulder surfing (Pham et al. 2014).

Possession factors are physical entities that the registered individual must have to access the network or system i.e., information that an individual can carry physically with them such as security token or mobile phones (Souza et al. 2017). Physical tokens are the most commonly used possession factor of authentication. The other example includes security tokens, smart cards, one-time password (OTP), and wireless tags. The tokens require special readers and can suffer from duplicity, stealing hacking, or damaging issues (Kwong et al. 1992). Inherence factors validate the identity of a user by using a unique physiological or behavioral characteristic of the requesting user and are usually known as biometrics characteristics. The various biometric characteristic includes iris and retina, face, fingerprint, palm print, DNA, which are physiological

identifiers while signature, voice, gestures, and gait are the behavioral identifiers. The biometric-based authentication system acquires a biometric key (e.g., fingerprints, faces, irises, hand geometry, palm prints, etc.) from an individual, extracts a feature set, stores it, and compares it with the stored database for accessing the system. If the two feature sets are matching, the system could recognize the individual; otherwise, the system will reject the individual (Jain et al. 2004). Since no system is secure therefore biometric-based authentication also has some drawbacks. Face and iris can be photographed, voices, and fingerprints can be spoofed, etc.

The performance of any authentication system is evaluated using two error rates i.e. false acceptance of impostors (FAR), and false rejection of genuine users (FRR) while the verification can be done based on parameters like equal error rate (EER) (Marcel and Millán 2007), and ROC curve (Fawcett 2006). The equal error rate describes the point where two error rates are the same i.e. FRR and FAR are equal (Marcel and Millán 2007). Receiver Operating Characteristics (ROC) is a graphical plot that provides a relationship between true positive rate (TPR) and false-positive rate (FPR) (Hitchcock 2003). No authentication system is fool-proof secured. The most common form of user authentication is the password. It is considered as an insecure form of authentication because they are easy to crack through online or offline means. Some popular mode of password attacks is brute force attack, dictionary attacks, and shoulder surfing. Physical tokens, such as smart cards or keys, may also be lost, stolen, or duplicated. Although, biometric-based authentication systems are generally safe but do have some issues such as spoofing the fingerprints or voice, and tricking an eye scanner, etc. Therefore, the current methods have exposed their security weaknesses (Pham et al. 2014). Many authentication studies recommend different ways to boost the security of passwords (Forget et al. 2008), for example, user security training, and implementing password policies that prevent users from using common words and repeated patterns (Blocki et al. 2013). But recent studies as mentioned above reflect some of the challenges in password-based, token-based, and biometric-based authentication systems.

To solve these issues, many research groups have suggested brain signals as a new authentication alternative for developing security systems. In recent studies, it has been demonstrated that the brainwave pattern for each individual is unique as well as almost impossible to duplicate, and therefore, can be used for authentication purposes (Paranjape et al. 2001). Also, such biometric traits naturally require alive person recording, which enhances the security of a traditional biometric-based (fingerprints, iris, etc.) system. The main advantage of using brain signals as an authentication identifier is that it is fraud-resistant.

Therefore, in recent years, Brain–Computer Interface (BCI) has emerged as a potential biometric modality.

Brain–Computer Interface (BCI) is a pattern recognition system that classifies every pattern into a category by its extracted capabilities. It is a multidisciplinary field; scientists from neuroscience, physiology, building, software engineering, restoration, and other specialized and medicinal services controls are occupied with this area (Ahirwal and Londhe 2012). In recent years, BCI emerges as a promising biometric modality with the benefits of being hard to fake or mimic, as an extracted signal is confidential because it corresponds to a secret mental task that cannot be observed (Marcel and Millán 2007). The monitoring of brain activity can be accomplished using invasive and non-invasive techniques. Non-invasive methods are the ones in which the electrodes are directly connected to the scalp there hence the quality of neural signals is relatively low as compared to invasive techniques (Liarokapis et al. 2014). The various non-invasive methods include magneto-encephalography (MEG), functional magnetic resonance imaging (fMRI), positron emission tomography (PET), optical imaging, and electroencephalography (EEG) (Vaughan et al. 2003). Easy access to signals, portability, low-cost involvement, features high temporal resolution and the availability of easy post-processing techniques result in consideration of EEG as the most prevalent recording modality in BCI (Wolpaw et al. 2002).

Brain–Computer Interfaces are designated according to the type of brain activity used for monitoring. Previously, researchers have studied, several EEG-based BCIs including, P300 potential (Farwell and Donchin 1988), steady-state visual evoked potential (SSVEP) (Lin et al. 2006), event-related de-synchronization (ERD), and slow cortical potential (Cecotti 2011). Evoked potentials are electrical signals generated by the subject when he/she receives outside stimuli (Shashibala and Gawali 2016). The outcomes obtained from evoked potentials are being averaged with a presentation of repeated stimuli as the amplitude of potentials measured is small. The well-known evoked signals are Steady-State Visual Evoked Potentials (SSVEP) and P300 potentials and commonly used stimuli are visual (e.g., a flash of light), auditory (sound related), and sensory (Rak et al. 2012). Development of BCI relies upon the selection of signals, data acquisition methods, and feature extraction methods, development of training strategies, protocols, and choice of application and user group. In this paper, P300 is used as the control signal for the development of BCI based authentication system. The P300 ERP is a positive deflection in the EEG signal that appears almost 300 ms after, the subject is exposed to the infrequently occurring or surprising tasks. This signal is usually generated through an “odd-ball” paradigm where the user is asked to attend a random sequence of stimuli in which one

is much less frequent than the other (Ramadan and Vasiliakos 2017). At whatever point relevant stimuli appear on the screen, it triggers the P300 signals of the user. The main advantage of using P300 is that it doesn't require training of the subject, but it requires repetitive stimuli for better outcomes (Arslan et al. 2016).

The P300 based paradigm was first developed in 1988 by Farwell and Donchin (1988). In this paradigm, users were presented with a set of 36 characters (alphanumeric) arranged in  $6 \times 6$  matrices. Each row and each column of the matrix flashes in random order. Subjects were instructed to select one of the alphabets or numbers of their choice. Further, subjects were asked to count the number of times the selected character was intensified while ignoring flashes of the adjacent characters. Whenever row and column of the selected character intensify simultaneously, a P300 signal is evoked that differentiates target from non-target character (Kellicut-Jones and Sellers 2018). Although, P300 speller is very effective in identifying the attended character with high precision. There is always a trade-off between accuracy and communication speed (Pan et al. 2013). It is also observed that adjoining rows and columns are the main source of error in the generation of target P300. Other factors influencing BCI performance includes concentration level, stress or anxiety, mental condition, etc.

All these factors create a need for the development of the modified P300 speller paradigm. Many efforts have been made in the past to enhance the performance of a P300 based BCI, including varying inter-stimulus interval (ISI) (Lu et al. 2013), matrix size (Sellers et al. 2006), flashing time, background colors (Salvaris and Sepulveda 2009), size of the character as well as inter-character distance (Salvaris and Sepulveda 2009) and implementing various methods of signal processing (Serby et al. 2005), etc. Guan et al. (2004), proposed the single character (SC) speller and compared its results with a row-column (RC) speller and observed that the SC speller can be used to achieve higher accuracy (Guan et al. 2004). The region-based (RB) stimulus was developed by Fazel-Rezai and Abhari (2009), to resolve the crowding effect of flashing icons that may cause errors when characters are spelled (Fazel-Rezai and Abhari 2009). The study showed better results in the RB speller configuration. McFarland et al. (2011) modified the conventional row-column paradigm and proposed a new checkerboard based paradigm. The proposed method flashes six different characters from random positions rather than flashing of row or column. The results showed improved accuracy and information transfer rate (ITR) (McFarland et al. 2011). Salvaris and Sepulveda (2009), examined the effect of background color, object size, and distance between the objects and found that white background produced the highest

accuracy while small-sized objects produced the lowest accuracy (Salvaris and Sepulveda 2009). Sellers et al. (2006), compared the performance of two different spellers by manipulating the matrix size ( $3 \times 3$  and  $6 \times 6$ ) and using different ISIs (175 ms and 350 ms). The results indicate that classification accuracy was highest for  $3 \times 3$  speller along with 175 ms ISI condition. But the amplitude of P300 was significantly greater for the  $6 \times 6$  matrix. It is because amplitude correlates with the probability of the oddball occurrence (Sellers et al. 2006). That means the magnitude of P300 increases with a lower probability of the occurrence of a target object (Donchin et al. 2000). Meinicke et al. (2002) in his study stated that reduced matrix size corresponds to the faster display of stimuli which improves the accuracy, and ITR of the system.

Overall, these researches have suggested many changes to the speller paradigm which may potentially increase the accuracy, bit rates, or both of the P300-Speller without increasing the error rates. But only a few research groups have concentrated on developing new flashing strategies to enhance the elicitation of visually evoked potentials in a BCI. Guo et al. (2008) developed a visual paradigm where objects move instead of flash to elicit ERP (Guo et al. 2008). Martens et al. (2009) proposed a FLIP stimulus. They proposed a paradigm in which gray rectangles were flipped horizontally instead of flashing characters to evoke ERPs (Martens et al. 2009). Furthermore, Kaufmann et al. (2011) and Zhang et al. (2012) determined that using changing human faces as visual stimuli in the P300-speller paradigm can substantially increase classification accuracy and the transfer rate of information. The prime purpose of this study was to develop a visual stimulus that allowed the subject to choose a password in terms of objects rather than characters. In the mentioned paradigm, pictures were replaced with new pictures with some delay of a few seconds. This varied from the conventional P300 paradigm in terms of elicitation, in this case, was found to be more significant (Kaufmann et al. 2011; Zhang et al. 2012). It has been already proved in previous studies that the elicitation using a face pattern are more pronounced as compared to only flashes (Kaufmann et al. 2011; Zhang et al. 2012).

In recent years, different research groups have proposed several authentication systems based on the brain signals but each study differs according to the methodology. Earlier studies mainly employed motor imagery (Marcel and Millán 2007), stimulus presentation, and performing mental computation for the development of the authentication systems (Palaniappan 2008). All authentication systems follow the same procedure i.e. acquisition of EEG data from an individual, storing recorded samples in the database, and comparing the EEG of the claiming user with those samples stored in the database. Paranjape et al.

utilized single-channel EEG, recorded for the identification of individual subjects during a simple eye closed/open task, and achieved an accuracy of 80% (Paranjape et al. 2001). Marcel and Millan suggested an authentication scheme based on inherent features and using models of Gaussian mixtures. Subjects were assigned to perform motor imagery and word generation tasks (Marcel and Millán 2007). R Palaniappan proposed a multiple thought identification model. The five mental tasks performed by the subjects are baseline task (relaxed state), geometric figure rotation, math task (digit multiplication), mental letter writing task, and visual mental counting (Palaniappan 2008). Thorpe et al. proposed a concept of pass thoughts similar to P300-BCI, a two-factor authentication system using a single user thought, which would have a unique signature even if another human was thinking something similar (factor one) and also be unique as a thought in the individual's mind (factor two). Since thoughts can represent anything (a word, phrase, image, emotion), the theoretical entropy of a passing thought is endless (Thorpe et al. 2005). Pham et al. introduced an EEG-based user authentication that has the combined advantage of both password-based and biometric-based authentication systems. In this multi-level security system, users were asked to provide EEG signals, and then not only their characteristics but also gender and age information was used to authenticate the user identity (Pham et al. 2014). Mu et al. proposed a paradigm using the stimuli of self-photos and non-self-photos. Randomly photos were displayed on a computer screen, and subjects were required to focus and classify each photo as self or non-self as accurately as possible (Mu et al. 2016). Seha et al. introduced a paradigm to improve the performance of the EEG based biometric authentication using eye blinking EOG signals which were considered as a source of artifacts for EEG. Participants used three different authentication tokens: relaxation (eyes closed), visual stimulations (using pictures), and eye blinking (EOG signals) (Abbas and Abo-Zahhad 2017).

This study aimed to design a BCI based authentication system with a higher classification accuracy, ITR, and reduced error rates by modifying the P300 speller: varying the matrix size ( $2 \times 2$ ), modifying visual stimulus presentation (pictures instead of characters), reducing ISI (175 ms), size of the character as well as inter-character distance (to avoid interference as well as fatigue), session recording (4 sessions), and classification technique (QDA). The proposed visual paradigm is a manipulated version of the conventional P300 speller ( $6 \times 6$  character matrix) developed by Farwell and Donchin (1988) with a difference that instead of characters, the speller consisted of pictures of different objects that are arranged in  $2 \times 2$  matrix. The interstimulus interval (ISI) of the proposed study also differs from the original study. The main



advantage of using a reduced size matrix is that overall run time also reduces as standard P300 speller ( $6 \times 6$  character matrix) requires 12 flashes for single character selection while the proposed  $2 \times 2$  speller needs only 4 flashes for single selection i.e. 3 times fewer flashes and hence, require less time for single target selection. It is evident from previous studies that ERPs elicited from famous faces would lead to improved classification accuracy (Henson et al. 2003). Therefore, in this study, pictures of different objects are used to stimulate a user's brain activity. Research on the P300 potential has shown that the shorter ISI yielded the highest classification accuracy (Meinicke et al. (2002); Sellers et al. 2006). Therefore, a novel BCI-based authentication system has been proposed which is based on the P300 evoked potentials that are elicited by a designed visual paradigm. Also, a detailed analysis of three classification techniques namely, Quadratic Discriminant Analysis (QDA), Quadratic Support Vector Machines (QSVM), and K-Nearest Neighbor (KNN) has been done.

The paper layout is as follows. The next section describes the data acquisition technique, description of the P300 speller paradigm, experiment layout, timeline, pre-processing and classification techniques, and performance evaluation. The results are summarized and discussed in the next section. Finally, concluding remarks are made in the final section.

## Material and method

EEG features contain a high level of uniqueness. However, a person forgets his/her ID cards, passwords, tokens, etc., but need not worry about forgetting or losing the EEG signal attribute. They cannot be changed and are difficult to mimic or compromise as signals regarding similar mental tasks are subject dependent (Lashkari et al. 2009).

### Participants

Ten university students (S1 to S10) had voluntarily participated in this experiment, out of which five participants were females. All the participants belonged to an age group of 18–30 (mean = 23 years) with normal or corrected to normal eyesight, and none of them had any neurological impairment history. Seven participants had no prior exposure to EEG recording. Subjects were instructed to avoid unnecessary movement and keep themselves relaxed during the experiment to prevent EMG artifacts from affecting the acquired EEG signal. The Institute Ethics Committee approved all the stimuli and experimental procedures.

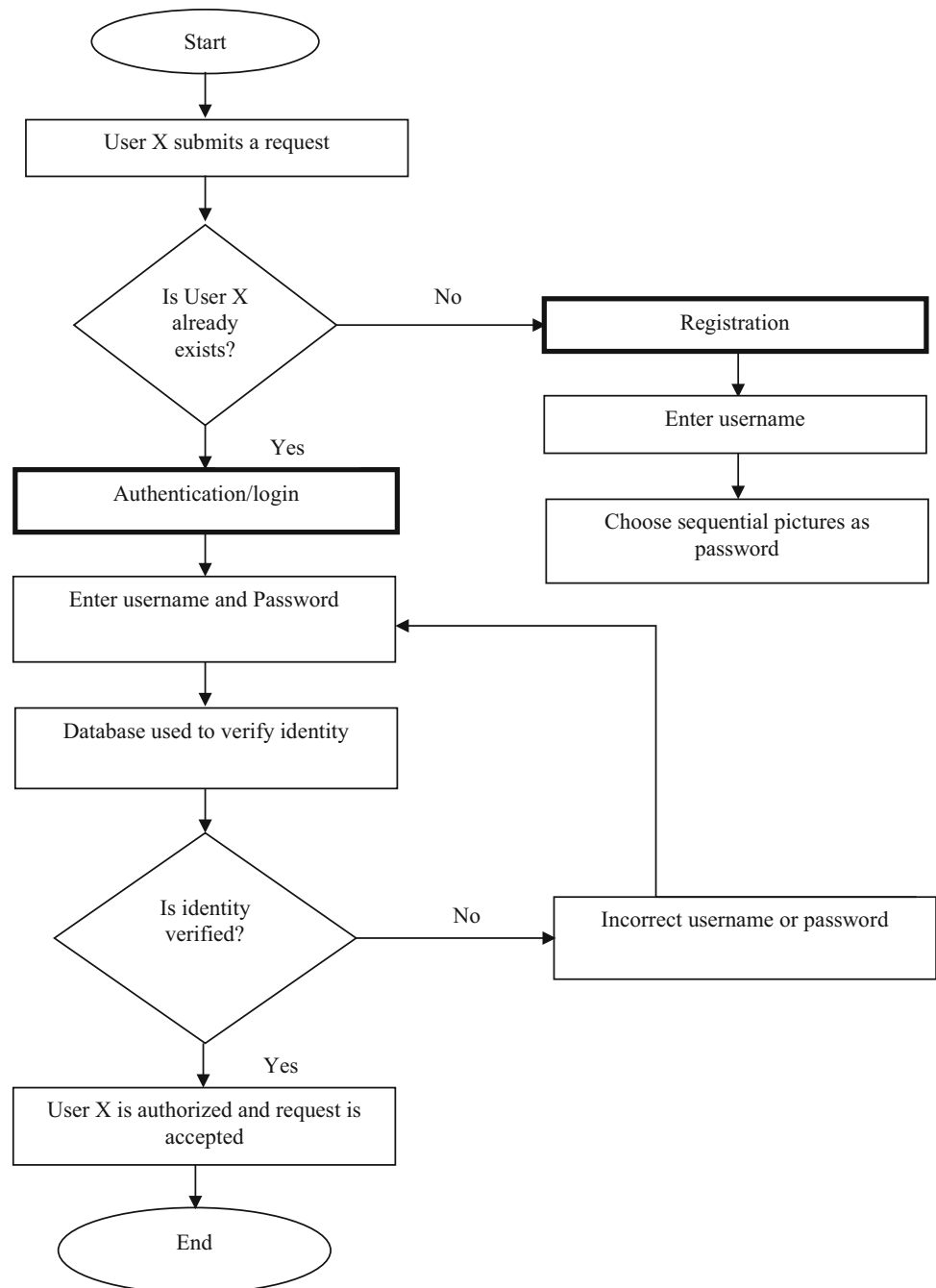
## Proposed layout

In the proposed work, pictures of various objects were displayed in a  $2 \times 2$  matrix. The rows and columns were flashed alternately in random order, while the user focuses on the specific picture, to choose it as their password pin. During this study, the term 'flash' is used to refer to the changing object picture that was just shown as a flash to elicit ERPs. During every trial, pictures from all the locations were changed at least once. For clarity, the authors use the term 'flash' to refer to these changes all through this paper.

P300 (ERP) was used to verify the identity of a claiming person with the help of randomized pictures of different items (like apple, chair, cat, etc.). For the P300 elicitation, large numbers of pictures of non-target objects were mixed with a small number of target pictures following an oddball paradigm i.e. subjects were required to focus on a rare event (target picture) by ignoring all other frequent events (non-target pictures). The client's brain reacts to the target stimuli and elicits a positive peak, which is known as P300. P300 occurs approximately from 250 to 400 ms after the appearance of target stimuli following the presented paradigm (Nicolas-Alonso and Gomez-Gil 2012; Artzi and Shriki 2018). Its amplitude may vary from person to person and with the type of stimulus used. We propose an authentication system using EEG signals as the primary attribute. The algorithm for the system is shown in Fig. 1. Our authentication system comprises two phases, i.e., Enrollment or Registration phase and Verification phase (Fig. 2).

In the *enrollment phase*, subjects were instructed to sit comfortably in a chair approximately 70 cm away from the screen (17" display) having a resolution of  $1600 \times 900$  pixels and refresh rate 60 Hz. After that, a database of 48 pictures of different objects was presented to the subject for password pin selection. The subjects were asked to select four pictures of their choice as a password. Subjects were asked to relax and avoid unnecessary movement during the data recording. For each pin selection, each subject has to complete four runs i.e. each session consists of four separate experimental blocks. In every experimental block, rows and columns of the matrix flashed in a random order where the target picture (one at a time) was flashed along with the flashing of non-target pictures (11 pictures), and EEG signals associated with the tasks were recorded. That means each block is comprised of 12 pictures (one target and 11 non-targets). Complete recording for each subject was done on two separate days (two periods). In each period, two EEG sessions (morning and evening) of five minutes were recorded. Therefore, there are a total of 40 EEG events (10 subjects  $\times$  2 periods  $\times$  2 sessions). Once

Fig. 1 Algorithm of paradigm



the raw EEG was collected, various pre-processing techniques were used to remove artifacts or noise associated with the recorded data. The pre-processed data was then used to train the classification model. Since, the mental tasks themselves are proof of authentication, as every individual has a unique thought process. The device, therefore, stores the data obtained from the user (password pictures as well as the trained P300 model) and labels them with the user's identity.

In the *verification phase*, whenever an unknown user wants to access the security system, elicitation of an EEG

signal is mandatory similar to which has been created earlier in the registration stage by repeating the same mental tasks as performed during the enrollment phase. The recorded EEG data set is pre-processed and the features extracted in the same way as in the enrolment phase. The obtained attributes of a claiming person are fed into the classifier for validation of data and compared with the data collected in the enrollment phase; if it matches the stored data, access is granted to the user. While the mismatching of these attributes denies access to the user. In other words, the proposed authentication system generates

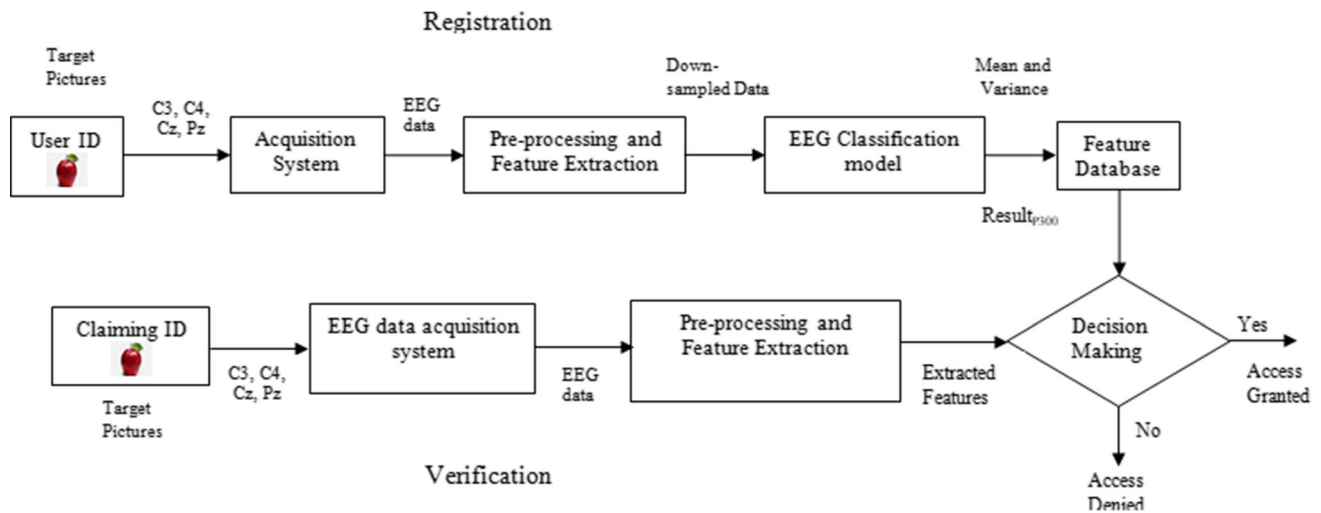


Fig. 2 Registration phase and login phase

a match score by comparing the EEG signals of a claiming person with the data set stored in the enrollment phase. The closer the match, the greater would be the match score. A threshold is used to control the decision-making process. If the matching score of claimed identity exceeds or equals to a threshold, then the user is genuine (accepted) otherwise, claiming ID is an imposter (rejected).

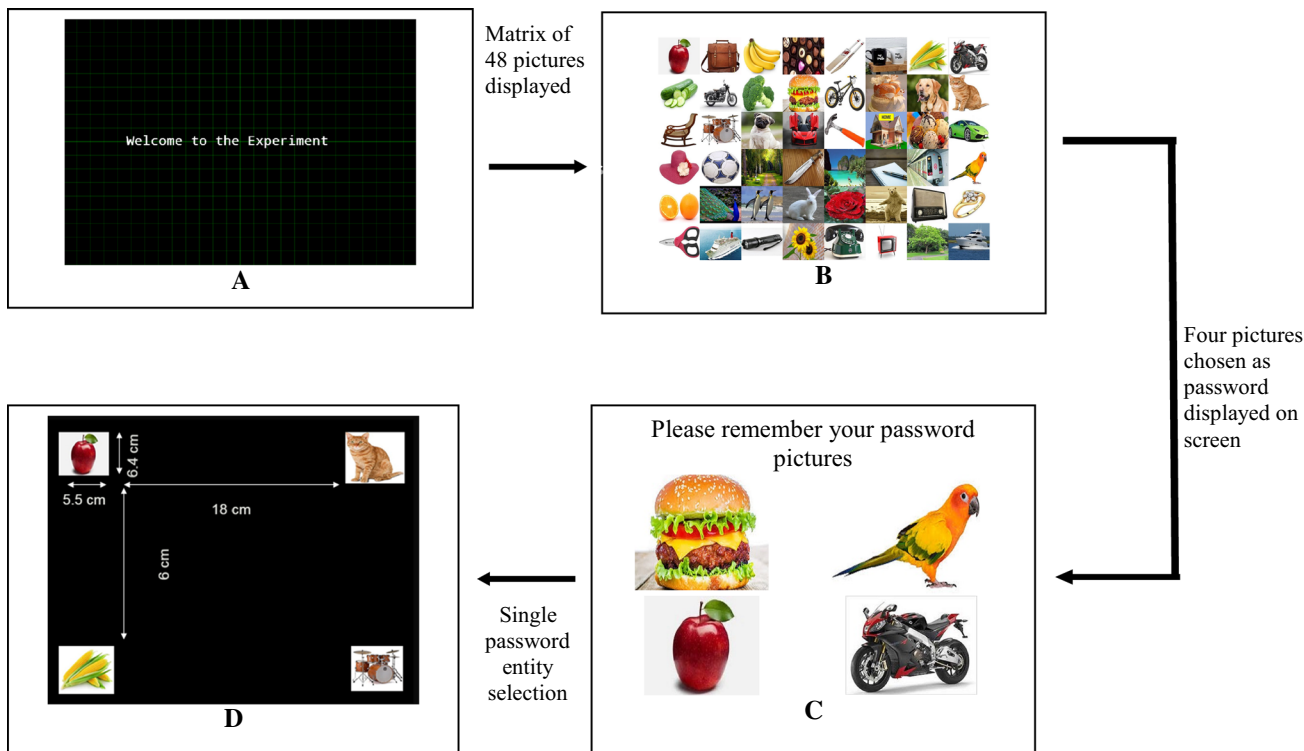
The performance of a proposed authentication system is evaluated using two error rates i.e. false acceptance rate (FAR) and false rejecting rate (FRR). These two parameters have been regulated by a threshold adjustment. If the threshold is set too high then valid users will be rejected i.e. FAR is reduced and FRR increased and if it is kept very low, then it authenticates the fraudsters i.e. FAR is increased and FRR reduced. Therefore, the value of the threshold would be kept somewhere in between the two. In this study, EER is used as a threshold set to evaluate the performance of the system. It is an algorithm that is used to determine the threshold values for its false acceptance rate and false rejection rate i.e. the point at which FAR and FRR are the same (Cheng and Wang 2004).

## Paradigm design

In the proposed paradigm, each row and each column of the alphanumeric matrix (characters and digits) is replaced by the pictures of different objects. The matrix flashing rate of the proposed speller is 5.7 Hz. The horizontal and vertical distance between the adjacent images is 18 cm and 6 cm respectively. The size of each picture is 6.4 cm × 5.5 cm. The flow chart of the experimental setup is shown in Fig. 3. During EEG recording, a 2 × 2 matrix consisting of pictures of different objects is presented on the computer screen placed in front of the subject, where rows and

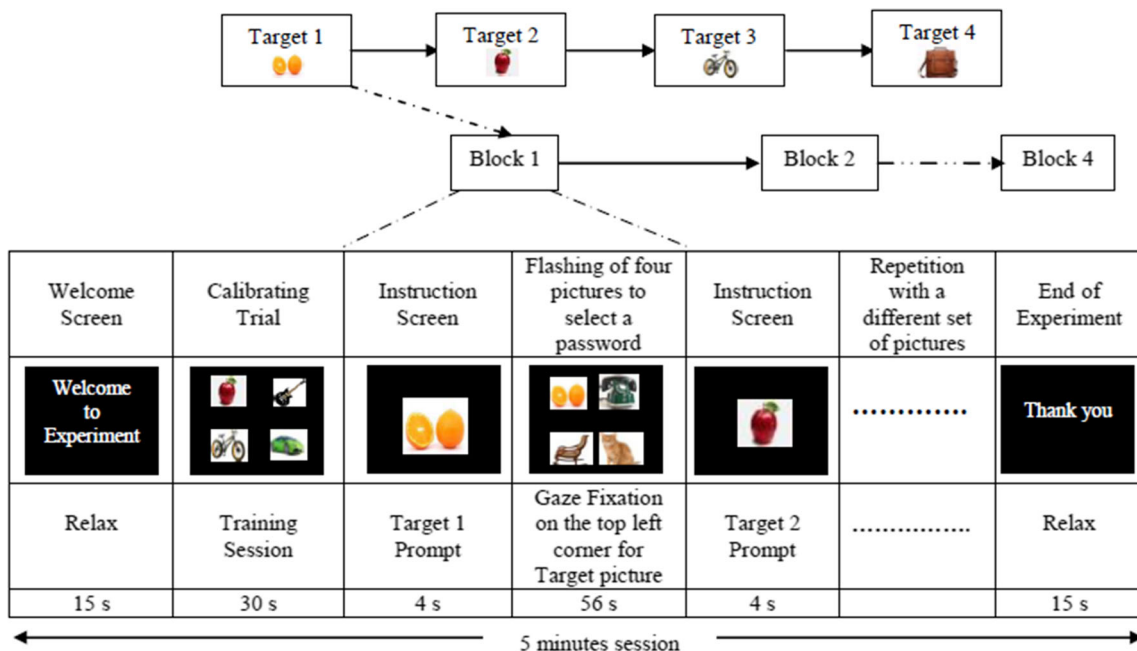
columns of this matrix are flashed consecutively in random order. To choose a target picture, the subject has to concentrate on the specific cell of the matrix. Therefore, any flash containing the cell on which the subject is primarily focused will result in a P300. The set of 4 flashes, 2 rows, and 2 columns, are required to highlight (intensify) a single picture once.

The *timeline* for the session is shown in Fig. 4. Each subject was exposed to a different set of images. The recording was done in four different sessions in a controlled environment; each session lasted for five minutes. The experimental protocol starts with a welcome screen followed by the database consisting of 48 pictures that are loosely based on Snodgrass and Vanderwart's picture set (Snodgrass and Vanderwart 1980) shown on a computer screen. The subjects can choose password pin (pictures) of their choice from this database. This trial lasted for 15 s followed by a calibrating trial that lasts for 30 s. In the calibrating trial, the subjects were asked to perform three different tasks: a relaxing task to standardize the baseline rhythm by performing no mental task and avoiding any movement for 5 s, horizontal eye movement to detect eye movement artifacts by moving their eyeballs from right side to left side for next 5 s, and for last 20 s, training trial was run to make a subject familiar with the visual stimulus paradigm. The next four minutes were segmented into 4 blocks of 60 s each, where each subject will face the proposed P300 based speller to perform a mental task. Each block is dedicated to a particular target picture (password pin) selection. During EEG recording, the target picture (low probability) was mixed with non-target pictures (high probability) arranged in a 2 × 2 matrix where rows and columns of the matrix were flashed consecutively in random order. Each block contains 12 pictures (one target and



**Fig. 3** Flowchart of paradigm. **a** Trial of the experiment starts with a welcome screen, **b** user chooses four pictures as his/her password from the database of 48 pictures, **c** chosen pictures for the password are displayed on the screen for confirmation. **d** Each subject is

presented with a proposed  $2 \times 2$  P300 speller where selected pictures (including non-target) are presented in rapid succession on four corners of a monitor screen. Each row and column intensifies for 100 ms every 175 ms



**Fig. 4** Detailed timeline for the session

eleven non-targets) presented at four corners of the screen, and the subject was instructed to focus on a specific target location to select a picture. In this work, the conventional

character flashing concept is replaced by a novel picture flashing concept where instead of characters, pictures of different objects were flashed in a randomized order.



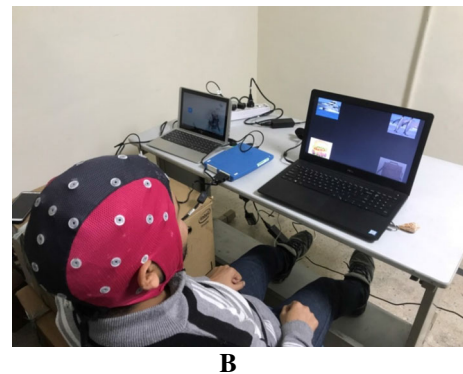
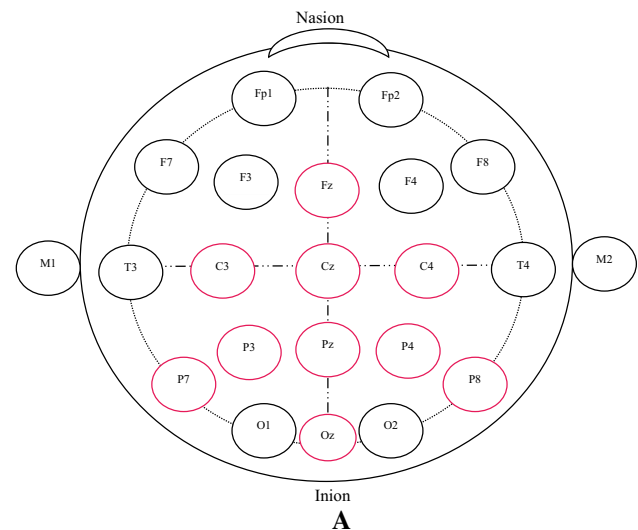
In a single experimental block, each picture was shown for 100 ms at the four corners of the computer screen followed by the black screen for 75 ms (175 ms ISI) i.e., a flash sequence lasts for 700 ms. Sellers et al. (2006) demonstrated in his study that short inter-stimulus time (175 ms) yield better performance results than the longer interval (350 ms). For every flash sequence, 4 pictures are chosen in a predefined manner from a set of 12 and presented at the four corners of the computer screen. Now subject was instructed to concentrate on a specific picture while fixing his/her gazes at the top left corner. This sequence occurred 80 times in a minute accounting to 56 s, succeeded by a target instruction screen of 4 s. The target picture appeared at a target location at least 5 times for each subject. Lastly, the subject was instructed to blink his/her eyes for 5 s to detect artifacts related to eye blinks. The last 10 s were dedicated to a resting state where no picture was displayed on the screen.

### EEG acquisition

During EEG acquisition, the signals from the required locations were recorded with the help of the eego™ Sports amplifier (ANT Neuro, inspiring technology, The Netherlands) with a maximum sampling rate of 2048 samples per second and a resolution of 24 bits. It has high input impedance ( $> 1 \text{ G}\Omega$ ) and high CMRR ( $> 100 \text{ dB}$ ). It has 32 referential channels, which are by default referenced to  $\text{CP}_z$ . All impedances were maintained below  $5 \text{ k}\Omega$  (Nicolas-Alonso and Gomez-Gil 2012). EEG data were recorded at a sampling rate of 512 Hz based on the international 10–20 system standardized by the American Encephalographic Society as shown in Fig. 5a (Nicolas-Alonso and Gomez-Gil 2012; Kosti et al. 2018). In EEG recording, only 10 electrodes were utilized, data from which was further amplified and digitized.

### Preprocessing and feature extraction

The fundamental goal of a P300 based algorithm is to distinguish target signals from non-target signals. Since P300 peak amplitude can be recorded best at parietal and central electrodes (Picton 1992), therefore, signals were acquired from  $\text{C}_3$ ,  $\text{C}_4$ ,  $\text{C}_z$ ,  $\text{F}_z$ ,  $\text{O}_z$ ,  $\text{P}_3$ ,  $\text{P}_4$ ,  $\text{P}_7$ ,  $\text{P}_8$ ,  $\text{P}_z$  electrode locations in terms of referential potential ( $\text{CP}_z$ ) (Kaongoen et al. 2017). The experimental setup and recording of EEG via eego™ Sport EEG acquisition amplifier are shown in Fig. 5b. The recorded information was pre-processed to diminish noise and artifacts. Preliminary processing was done by Advanced Source Analysis (ASA) software provided by the ANT Neuro, where a sixth-order Butterworth band-pass filter was used to filter the EEG between 0.1 and 30 Hz. The baseline correction was carried out on the



**Fig. 5** **a** The electrode montage used in this study based on the International 10–20 Electrode system. The ten electrodes selected for analysis are highlighted. **b** The experimental setup comprises of two laptops, a 32 electrode cap, and one recording amplifier. The first laptop is used for data recording monitoring (on left) connected with an eego™ Sport EEG acquisition amplifier (blue color device), while another is used for stimulus presentation (on right)

calibration trial's first five seconds (base rhythm recording). This approach subtracts the DC offset by measuring the mean over the baseline period and subtracts this mean from the EEG in the correction period specified to the event. The EEG recorded at the time of eye movement (5 s), and eye blinks (5 s) was utilized for artifact removal. The Principal Components Analysis (PCA) method is utilized for the determination of topographies of the brain signals free from artifacts like eye blinks (Ille et al. 2002). For this, the following two data topography parameters were to be specified: maximum allowed magnitude and maximum correlation with artifact subspace. High amplitude artifacts above the normal amplitude range of the EEG ( $100 \mu\text{V}$  considered in this study) are identified. Only 50% of the spatial correlation between the data segment and the artifact segment was allowed for differentiating brain signals from artifacts. The relative power of signal control

obtained was greater than 95% in all cases with only one PCA component.

Furthermore, time-domain features are derived which is correlated with changes in the amplitude of the signal occurring during the stimulus presentation. Since the experiment setup consists of four blocks (i.e. one block for single target selection) of one minute each, the recorded datasets were therefore segmented into a minute window. As explained in the above section, for each subject the target picture appears at least five times in one block. Thus, the data acquired from each electrode were segmented into five epochs for target picture selection by applying a time window of 1 s (512 samples) from the start of the stimulus onset. This protocol was separately implemented for non-targets. Hence, ten epochs (5 targets and 5 non-targets) were obtained from single block, in total 40 epochs (4 runs  $\times$  (5 targets + 5 non-targets)) from four blocks. The obtained data samples were down-sampled to reduce the size of feature vectors using the Chebyshev Type I low pass filter. Furthermore, normalization was done to have a zero mean, and unit variance and data were scaled to the interval of  $-1$  to  $1$ . The preprocessing technique used resulted in a feature vector of 320 (i.e.,  $(512 \times 1)/16$  samples  $\times$  10 channels) elements for single target or non-target selection. Since complete experimental data for one session comprised of 40 epochs, therefore finally constructed feature vector has a length of 12,800 elements ( $400 \times 32$ ), and the whole data for one subject consisted of 51,200 ( $1600 \times 32$ ) elements.

## Classification method

The technique of feature classification helps in the user's intentions based decision making in terms of feature vectors. The classification consists of two processes; the training process which is to learn and the testing process, which is to assign the class (Han et al. 2012). In this study, five-fold cross-validation was used to estimate the average classification accuracy for each subject. More specifically, the 80% data from each recording session was used to train a classifier and the left-out data (20%) from the session was used for testing. Further, data from session 1 was cross-validated with the data from sessions 2 i.e., training data from session 1 was used to train the classifier and testing data from session 2 was used for testing and vice versa. This cross-validation procedure was repeated across the sessions. The training data set contained 1280 randomly selected epochs which are used to build and train the model while testing data sets consisted of the remaining 320 epochs used for performance evaluation. The impact of different machine learning algorithms on classification accuracy was evaluated in an offline mode. Three classification methods: Quadratic Discriminant Analysis (QDA),

Quadratic Support Vector Machine (QSVM), and K-Nearest Neighbors (kNN) are compared for classifying EEG data. The classification results indicate that QDA provides the best overall performance.

On considering the testing data of this study, it was found that Quadratic Discriminant Analysis (QDA) outperformed all the other classification algorithms based on accuracy. In this study, quadratic discriminant analysis (QDA) is used as the classification tool, which is a simple probabilistic classifier with reasonable accuracy.

*Discriminant analysis* works under the supposition that each class pursues a Gaussian distribution. That is, for each class, the likelihood of appropriation can be displayed by:

$$f_K(x) = \frac{e^{(-\frac{1}{2}(x-\mu_K)^T \Sigma_K^{-1}(x-\mu_K))}}{(2\pi)^{p/2} |\Sigma_K|^{1/2}} \quad (1)$$

where  $x$  is the feature vector,  $\mu_K$ , and  $\Sigma_K$  denotes the mean vector and the covariance matrix of a given class, respectively.  $\Sigma_K$  and  $\Sigma_K^{-1}$  represent the determinant and inverse of the covariance matrix, respectively,  $p$  represents the number of features.

Let  $\pi_K$  represents the probability of membership in the previous class. Application of Bayes Theorem (Duda et al. 2001) results in:

$$p(K = k|X = x) = \frac{f_k(x)\pi_k}{\sum_i f_i(x)\pi_i} \quad (2)$$

Noting that probabilities are non-zero and the natural logarithm is monotonically increasing; the following rule can be used for classification:

$$\arg \max_k \frac{f_k(x)\pi_k}{\sum_i f_i(x)\pi_i} = \arg \max_k \log(f_k(x)) + \log(\pi_k) \quad (3)$$

The application of the natural logarithm helps to simplify the classification rule when working with a Gaussian distribution. The resulting sets of functions  $\delta_K$  are known as discriminant functions.

Quadratic Discriminant Analysis (QDA) uses a covariance matrix, which must be estimated for each class  $k$ , i.e.; QDA does not make the simplifying assumption that each class shares the same covariance matrix. This results in a quadratic classifier in  $x$ :

$$\delta_k(x) = -\frac{1}{2}(x - \mu_K)^T \sum_k^{-1} (x - \mu_K) - \frac{1}{2} \log \left( \left| \sum_k \right| \right) + \log \pi_k \quad (4)$$

The *K-Nearest Neighbor (KNN)* classifier is based on the principle that features belonging to the different classes will generally form separate clusters in the feature space, whereas the close neighbors with similar properties belong to the same class (Nicolas-Alonso and Gomez-Gil 2012).

All feature vectors obtained from the sub-training set are placed within the feature space. A feature vector that belongs to the test data is identified by the class of most k-nearest neighbors of all the located feature vectors. The performance of the nearest neighbor classifier depends on the distance function and the value of the neighborhood parameter k, which regulates the neighborhood volume (Kayikcioglu and Aydemir 2010). The advantage of considering k neighbors in the classification is that the probability of error in the decision making is reduced. The Euclidean metric is the most common choice for distance function.

$$\text{Distance (d)} = \sqrt{\sum_i^n (p_i - q_i)^2} \tag{5}$$

where  $p_i$  (or  $q_i$ ) is the coordinate of p (or q) in dimension i and d is the Euclidean distance.

The *Support Vector Machines (SVM)* are one of the most popular multi-class classification methods for high dimensional feature vectors. The technique aims to find a hyperplane in the feature space to maximize the distance between this hyperplane and the nearest data point of each class (Borges 1998). Consider a training set of N points with class labels as  $y_i \in [\pm 1]$ . The following quadratic programming problem is solved for the construction of the optimal separating hyperplane with maximum margin and minimizing the classification error ( $\xi$ ).

$$\min_{w, \xi} \left[ \frac{1}{2} \|w\|^2 + C \sum_{i=1}^N \xi_i \right] \tag{6}$$

where w is the weight vector and C is the regularization parameter. The regularization parameter is a user-defined parameter used to control the amount of permitted overlap between classes (Kayikcioglu and Aydemir 2010). The SVM can be categorized as linear and non-linear classifiers. In linear SVM, data is classified with the help of hyperplane while non-linear classifiers use kernels to make non-separable data into separable data. There are several kernel functions including linear, polynomial, Radial Basis Function, and sigmoid. Non-linear SVM results in more robust decision boundaries in the data space, which can improve the classification accuracy.

### Performance evaluation

Information Transfer Rate, error rates, precision, accuracy, and F1-score can evaluate the performance of the BCI system. ITR is used to evaluate the communication performance of BCI systems (Wolpaw et al. 2002). For a trial with N possible choices in which each alternative is equally probable, the accuracy (Acc) that the desired option will indeed be selected remains invariant and each error choice

has the same probability of selection. The ITR (bit/min) can be calculated as:

$$B = \log_2 N + \text{Acc} \log_2 \text{Acc} + (1 - \text{Acc}) \log_2 \text{Acc} \frac{1 - \text{Acc}}{N - 1} \tag{7}$$

$$\text{ITR} = B \times \frac{60}{t} \tag{8}$$

where B denotes the bit rate of determining one target; t denotes the time of deciding one target. The framework assessed with two error rates i.e. False Acceptance Rate (FAR) that occurs when a subject who should be rejected is accepted by the system and False Rejection Rate (FRR) which is defined as a measure of the chance that a subject who should be accepted is rejected by the system (Araújo et al. 2005). The following formulas are used:

$$\text{FAR} = \frac{\text{Number of false acceptances}}{\text{Total number of imposter attempts}} \tag{9}$$

$$\text{FRR} = \frac{\text{Number of false rejections}}{\text{Total number of genuine user attempts}} \tag{10}$$

From a security perspective, the FAR framework preferred over FRR on the ground that FAR acknowledges false personalities. An ideal authentication system should have a low value of FAR and FRR but practically often needs to make a trade-off between the two parameters. Therefore, the system sets a threshold to determine whether to allow or refuse any incoming request. The performance of an authentication system is evaluated using an equal error rate (EER) which is the point on the ROC curve where FAR and FRR cross i.e. values of two error rates become equal (Cheng and Wang 2004). ROC reveals interdependencies between sensitivity and specificity (Narkhede 2018). The ROC curve is plotted with the sensitivity (TPR) on the y-axis and 1 – specificity (FPR) on the x-axis. This study also examines the use of the area under the ROC curve (AUC) as a performance index of classifiers (Streiner and Cairney 2007).

Sensitivity, also known as recall, of a test is its ability to determine the authorized cases correctly. The specificity of a test is its ability to determine unauthorized cases correctly.

The sensitivity (SE) and specificity (SP) can be calculated from the given formulas (Oweis et al. 2013):

$$\begin{aligned} \text{Sensitivity (Sen)} & \\ &= \frac{\text{True Positives (TP)}}{\text{True Positives (TP) + False Negatives (FN)}} \end{aligned} \tag{11}$$

$$\begin{aligned} \text{Specificity (SPE)} & \\ &= \frac{\text{True Negatives (TN)}}{\text{True Negatives (TN) + False Positives (FP)}} \end{aligned} \tag{12}$$

where true positive (TP) denotes the EEG signals classified as target elicited by the chosen password pictures; true negative (TN), denotes the EEG signals classified as non-target elicited by the non-password pictures; false negative (FN), denotes the EEG signals classified as non-target elicited by the password pictures; false positive (FP), denotes the EEG signals classified as target elicited by the non-password pictures. Successful systems will have high True Positive and True Negative values while a poor or weak system will have high False Positive and False Negative values.

Precision provides the proportion of true positives relative to the number of predicted positives. That means, it is used to test the certainty of the prediction model, whether, predicted authorized cases are authorized or not. While the F1 score summarizes both precision and recall and can be understood as the harmonic mean of the two measures. An F-score of 1 indicates perfect precision and recall, therefore the higher the F1 score, the better is the model (Zeynali and Seyedarabi 2019).

## Results

All the subjects completed all the scheduled runs across the sessions. The pre-processed EEG data recorded from the central and parietal locations of each subject were averaged over 80 accurate detections for both target and non-target stimuli. A repeated-measures analysis of variance (ANOVA) was used to investigate the effects of the various classification techniques on the performance outcomes. Table 1 shows the performance comparison of the proposed paradigm with the previous works whereas; Table 2 provides the classification performance results of three classifiers, clearly showing the superiority of QDA. Table 3 provides the subject-wise performance of Day 1 recording. Further a statistical analysis was performed using a paired *t*-test to determine whether or not the two-period recording (Day 1 and Day 2) have any significant difference in performance based on average classification accuracies, ITR,

**Table 2** Average accuracy and ITR of the various classifiers based on the proposed paradigm

Classifiers	Accuracy (%)	ITR (bits/min)
QDA	97.0	37.14
QSVM	83.46	31.73
KNN	74.56	29.68

FAR, etc. Table 4 provides information about the classification performance of Day 1 and Day 2.

Detection of the target pictures from a set of EEG trials is based on the amplitude variations between target and non-target sample waveforms. P300 waveform of electrode  $C_3$ ,  $C_4$ ,  $C_z$ , and  $P_z$  were shown in Fig. 6, where the blue line indicates the appearance of the target picture, and a red line indicates the absence of target (only non-target displayed). Also, the difference in P300 amplitudes for target and non-target stimuli at different electrode sites averaged across all participants was statistically validated using analysis of variance (ANOVA). The comparison between the maximum amplitude in selected samples from the EEG data was made by setting the null hypothesis that the means ( $\mu_{\text{target}} = \mu_{\text{non-target}}$ ) of the maximum amplitude is statistically equal for both data set (target and non-target). The null hypothesis will be rejected if a higher maximum amplitude appears in the target condition than in non-target conditions. The target condition elicited a clear P300 with the largest amplitude at  $C_z$ ,  $P_z$ , and other electrode locations. The output of ANOVA confirmed high significance ( $F$ -value = 6.329,  $p = 0.014$ ) and ( $F$ -value = 5.242,  $p = 0.025$ ) for electrodes  $C_z$  and  $P_z$  respectively. Hence, the null hypothesis for  $C_z$ ,  $P_z$ , and other electrodes are rejected with a  $p$ -value of less than 0.05 ( $p < 0.05$ ).

The average accuracies obtained with QDA, QSVM, and KNN for all subjects are 97.0%, 83.46%, and 74.56%, respectively while the average information transfer rates are 37.14, 31.73, and 29.68 bits/min, respectively. To compare the performance of the different classifiers statistically, a repeated-measures analysis of variance

**Table 1** Performance comparison of the previous works

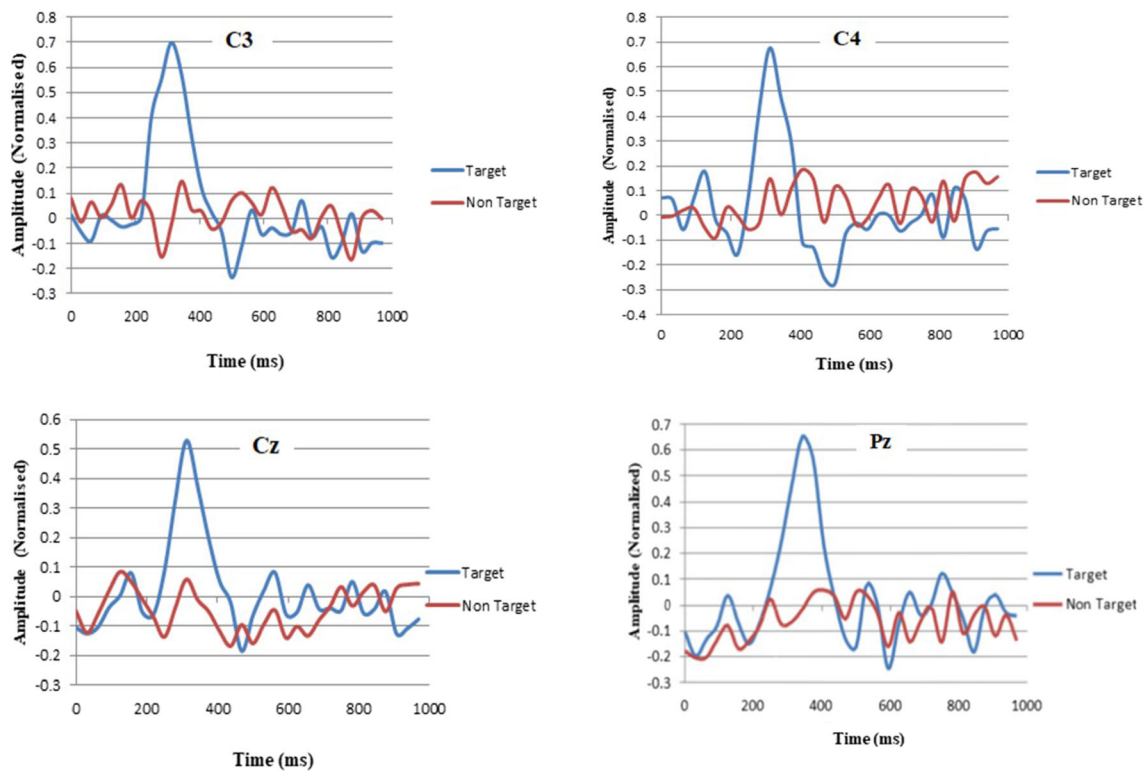
Authors (s)	Subjects	Type of stimulus	Electrodes	Accuracy (%)	FAR (%)	FRR (%)
Chen et al	16	Pictures	28 electrodes	87.8	$1.69 \times 10^{-4}$	–
Mu et al	10	Self- and non-self-photos	02 electrodes	87.3	5.5	5.6
Yeom et al	10	Visual stimuli (self and non-self faces)	05 electrodes	86.3	13.9	13.9
Wu et al	45	Face RSVP	16 electrodes	91.46	9.23	7.85
Proposed method	10	Different objects pictures	10 electrodes	97.0	2.77	3.21

**Table 3** Subject wise classifier performance on Day 1

Subjects	Accuracy (%)	ITR (bits/min)	FAR (%)	FRR (%)	Sensitivity (%)	Specificity (%)	F1-Score (%)	Precision (%)
S1	97.20	37.22	1.90	3.60	98.10	96.40	97.20	96.30
S2	97.90	37.49	1.90	2.30	98.10	97.70	97.80	97.60
S3	96.80	37.05	2.80	3.60	97.20	96.40	96.70	96.20
S4	95.80	36.71	3.70	4.50	96.30	95.50	95.80	95.40
S5	96.10	36.79	4.10	3.70	95.90	96.30	96.10	96.30
S6	98.40	37.68	1.40	1.80	98.60	98.20	98.40	98.10
S7	95.20	36.47	5.10	4.60	94.90	95.40	95.10	95.40
S8	98.60	37.77	0.50	2.20	99.50	97.80	98.60	97.60
S9	94.90	36.39	4.70	5.40	95.30	94.60	94.80	94.40
S10	97.70	37.40	2.80	1.80	97.20	98.20	97.70	98.10
Average	96.90	37.09	2.98	3.35	97.10	96.70	96.80	96.60

**Table 4** Classifier performance on Day 1 and Day 2

Day	Accuracy (Ac)	ITR	Precision (Pre)	F1-score (F)	Sensitivity (Sen)	Specificity (Spe)	FAR	FRR
Day 1	0.969	37.097	0.966	0.968	0.971	0.967	0.0289	0.0335
Day 2	0.971	37.188	0.969	0.971	0.973	0.969	0.0265	0.0307



**Fig. 6** Averaged potential elicited by targets (blue line) and non-targets (red line) on electrodes C<sub>3</sub>, C<sub>4</sub>, C<sub>z</sub>, and P<sub>z</sub> respectively

(ANOVA) test (with significance level  $\alpha = 0.05$ ) was conducted. The null hypothesis ( $H_0$ ) states that the means of classification accuracies and ITR are identical while an

alternative hypothesis ( $H_a$ ) suggests that means are not equal.

$$H_0: \mu_{QDA} = \mu_{KNN} = \mu_{SVM} \quad H_a = \mu_{QDA} \neq \mu_{KNN} \neq \mu_{SVM}$$



where  $\mu$  denotes the means of both parameters. The outcomes of the repeated ANOVA showed a considerable difference between the performance of the three classifier based on classification accuracy ( $F(2,27) = 125.483, p = 0.00001$ ) and ITR ( $F(2,27) = 151.951, p = 0.00001$ ). The results of the comparative study conducted can be summarised by Table 2 which suggests that QDA outperformed all the other methods in terms of both bit rates and accuracy. Figure 7 provides the box plot of classification accuracy (%), obtained for the different classifiers. Furthermore, the performance of the classification model is evaluated by the ROC curve and the AUC area. Figure 8

population 2 is defined as the performance characteristics from ten subjects processed on Day 2 with average means denoted by  $\mu_2$  ( $\mu_{2Ac}, \mu_{2ITR}, \mu_{2FAR}, \text{etc.}$ ).

To compare the results of the different parameters in different session recording statistically, a paired  $t$ -test (with significance level  $\alpha = 0.05$ ) was conducted. The null hypothesis ( $H_0$ ) states that the means of classification accuracies, ITR, FAR, etc. are identical while an alternative hypothesis ( $H_a$ ) suggests that means are not equal. The null hypothesis  $H_0$  and alternate hypothesis  $H_a$  for all the cases are defined below.

$$\begin{array}{ll}
 H_0: \mu_{1Ac} = \mu_{2Ac}; & H_a: \mu_{1Ac} \neq \mu_{2Ac} \\
 H_0: \mu_{1Pre} = \mu_{2Pre}; & H_a: \mu_{1Pre} \neq \mu_{2Pre} \\
 H_0: \mu_{1Sen} = \mu_{2Sen}; & H_a: \mu_{1Sen} \neq \mu_{2Sen} \\
 H_0: \mu_{1FAR} = \mu_{2FAR}; & H_a: \mu_{1FAR} \neq \mu_{2FAR} \\
 H_0: \mu_{1ITR} = \mu_{2ITR}; & H_a: \mu_{1ITR} \neq \mu_{2ITR} \\
 H_0: \mu_{1F} = \mu_{2F}; & H_a: \mu_{1F} \neq \mu_{2F} \\
 H_0: \mu_{1Spe} = \mu_{2Spe}; & H_a: \mu_{1Spe} \neq \mu_{2Spe} \\
 H_0: \mu_{1FRR} = \mu_{2FRR}; & H_a: \mu_{1FRR} \neq \mu_{2FRR}
 \end{array}$$

presents the performance comparisons of three students (S3, S8, and S9) based on ROC curves. The results obtained from the area under the ROC curve (AUC) for the three subjects are 0.968, 0.949, and 0.986 respectively.

The two-period recordings (Day 1 and Day 2) are compared based on the various performance parameters (like classification accuracy, ITR, FAR, etc.). To compare the results across the sessions, a paired  $t$ -test was performed since the parameters were so close in value (Table 4). Population 1 is defined as the performance characteristics from ten subjects processed on Day 1 using a single-step classification protocol with average means denoted by  $\mu_1$  ( $\mu_{1Ac}, \mu_{1ITR}, \mu_{1FAR}, \text{etc.}$ ). Similarly,

The mean accuracy rates for the proposed  $2 \times 2$  speller from the two-period recording are 96.9% and 97.1% respectively. The mean precision, and F1-score values are 96.6%, 96.9% and 96.8%, 97.1%, respectively, for the two days recording. The  $t$ -test results obtained from different sessions shows no significant variations in the accuracies [ $t(9) = -0.41153, p > 0.68554$ ], precision [ $t(9) = -0.4672, p > 0.645962$ ], and F1-score [ $t(9) = -0.4017, p > 0.692669$ ] respectively. Table 4 provides information about the mean classification accuracy, precision, and F-score yielded from Day 1 and Day 2

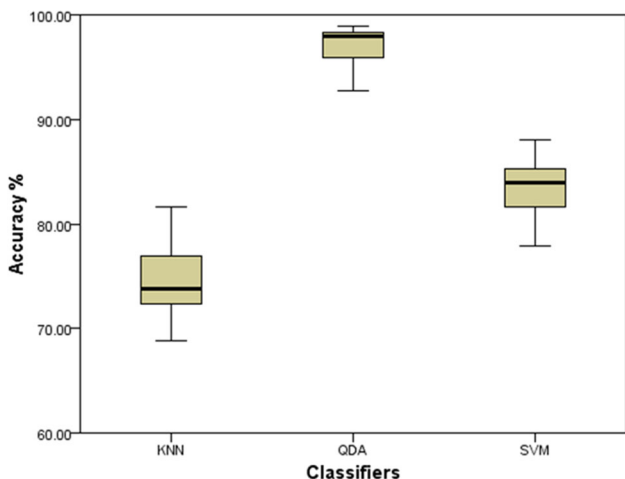


Fig. 7 Box plots of the accuracies obtained from the different classifiers (KNN, QDA, and QSVM)

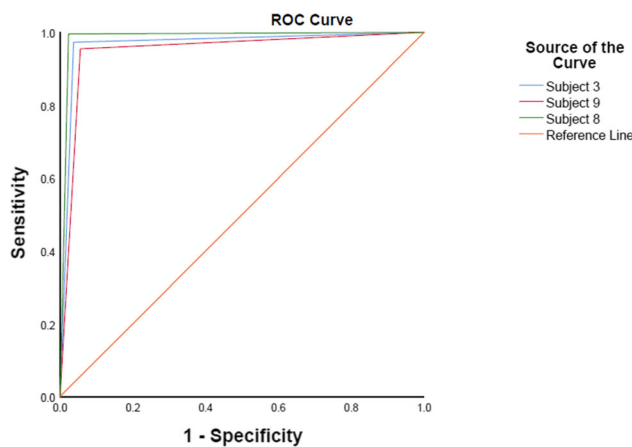
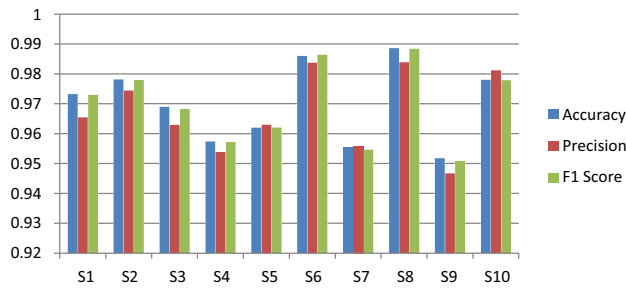


Fig. 8 Comparisons of receiver operating characteristic (ROC) curves for the three students based on classification results. Three ROC curves represent the performance levels of three students (S3, S8, and S9). Subject 8 clearly outperforms other two in terms of classification accuracy



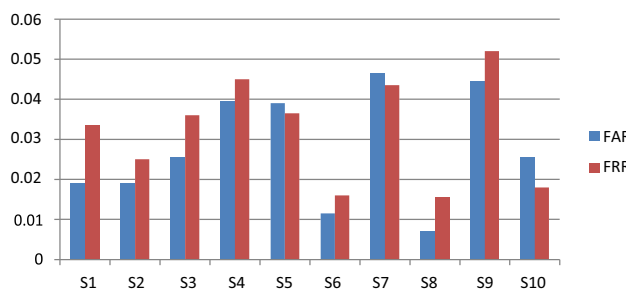
**Fig. 9** Averaged accuracy, precision, and F1 score of each subject (S1–S10) across the sessions

recording. Figure 9 shows bar plot of mean accuracies, precision, and F-score obtained from the recorded data from different sessions.

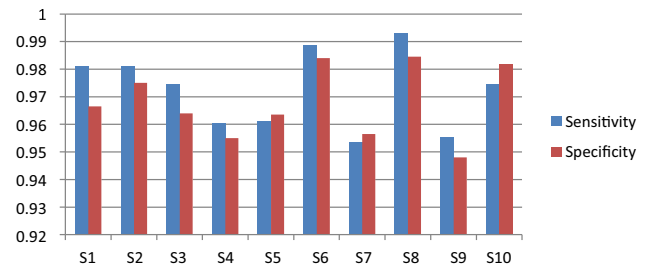
The mean ITR for the proposed  $2 \times 2$  speller across the sessions is 37.097 and 37.188 bits/min respectively. The results of the paired  $t$ -test for average ITR are  $t(9) = -0.4091$ ,  $p > 0.6872$ , which is greater than the significance level  $\alpha = 0.05$ . Therefore, no significant variations are found in ITR values from the session recording. Table 3 shows mean bits/min and associated mean accuracy for each period recording.

The mean FAR for the  $2 \times 2$  speller is 2.89% and 2.65% respectively whereas the mean FRR obtained from different sessions is 3.35% and 3.07% respectively. In case of FAR the paired  $t$ -test classifier yielded a result of  $t(9) = 0.37951$ ,  $p > 0.70875$  whereas in case of FRR results obtained are  $t(9) = 0.47551$ ,  $p > 0.640143$ . The  $t$ -test results indicate that session yielded no significant effects on error rates. Figure 10 shows the bar plot of mean FAR and mean FRR for each subject across the sessions. The results of this experiment with ten subjects showed a promising EER of 3.11% and 2.86% from two days of recording.

Figure 11 depicts the subject wise analysis of sensitivity, and specificity for P300 based authentication system. The sensitivity and specificity of the proposed method are 97.1%, 97.3% and 96.7%, 96.9%, respectively, for the two days recording. The session results shows no significant



**Fig. 10** Averaged FAR and FRR of each subject (S1–S10) across the sessions



**Fig. 11** Averaged sensitivity and specificity of each subject (S1–S10) across the session

variations in the sensitivity [ $t(9) = -0.37951$ ,  $p > 0.708753$ ], and specificity [ $t(9) = -0.47551$ ,  $p > 0.640143$ ] respectively.

Our proposed paradigm helps in achieving EEG based authentication with high accuracy of 97.0% and a bit rate of 37.14 bits/minute. Also, error rates (FAR and FRR) are 2.77% and 3.21% respectively. The other performance matrices also achieve high results; mean sensitivity of 92.2%, mean specificity equals to 96.8%, mean precision of 96.7%, and F1 score equals to 96.9%.

### Discussion

This study demonstrates the implementation of a new authentication scheme based on brain signals. Brain signals are advantageous because they can not be quickly duplicated, unlike other biometric features, such as face detection or iris scans. Furthermore, this research shows various significant points that can be very helpful in developing BCI based authentication system such as the reduced matrix size, visual stimulus, and smaller ISI can yield higher classification rates despite the increased likelihood of presenting the item being attended. Also, classification accuracy remains consistent throughout four sessions. Reducing the number of choices would result in increased character size shown on the screen, which would also maximize the distance between the two characters. Thus, a P300-based speller can also be used for visually disabled people as well as for those who have little control over their eye movements (Posner and Petersen 1990). The proposed authentication system yielded higher accuracy corresponding to the shorter ISI. This result is in line with the effects identified by the two previous studies (Meinicke et al. (2002); Sellers et al. 2006) on ISI. The average information transfer rate (37.14 bits/min) achieved was higher than the previous studies. Donchin et al. (2000) in his study achieved ITR of 20.1 bits/minute. In another study, the average transfer rate of 47.26 bits/min corresponds to an accuracy of 44% was achieved, which is not feasible in an actual BCI program (Meinicke et al. 2002).

The classification accuracy and bit rate obtained in the other studies as mentioned in Table 1 cannot be directly compared with those obtained in the present study because of variations in experimental paradigms and subject populations. However, it is possible to recognize many factors which may have caused the discrepancies. These factors are the classification algorithms, matrix size or number of choices, and ISI, etc.

Performance under each of the four sessions was investigated using a paired *t*-test. Four factors were considered in the analysis of the classification data, grid size ( $2 \times 2$  matrix) (Sellers et al. 2006), visual stimulus type (pictures of different objects), ISI (175 ms) (McFarland et al. 2011), and the number of sessions (4). Session results yielded no significant effects with  $p > \alpha$ , hence we accept the null hypothesis and reject the alternative hypothesis that the single-step classification on Day 1 (population 1) showed no significant difference in the performance parameters (classification accuracy, ITR, FAR, etc.) as compared to Day 2 (population 2) classification ( $\alpha = 0.05$ ).

Few research groups have analyzed the effect of grid size on classification accuracy and ITR. Allison and Pineda (2003) demonstrated that bigger matrices elicited a larger P300 amplitude since the probability of occurrence of a target item is reduced but the research did not analyze the classification accuracy hence it is unclear how their findings contribute to the selection of targets. Large size matrices required more flashes to detect a single target element, and hence, required more time for single entity selection as compared to a reduced size matrices. It leads to the slower speed of the BCI system (Allison and Pineda 2003). Sellers et al (2006), in his study, demonstrated that the overall accuracy was higher in the smaller matrix ( $3 \times 3$ ) condition than in the larger matrix ( $6 \times 6$ ) condition. The present research extends this result to show that the manipulation of probabilities to detect target items improves the classification accuracy (Sellers et al. 2006).

The current study reported that the shorter ISI (175 ms) achieved the highest classification accuracy. This finding is in line with the results obtained by Sellers et al. (2006) and Meinicke et al. (2002). They examined the impact of ISI on P300 accuracy and found that shorter ISI was usually correlated with higher accuracy and bit rates. As mentioned earlier, longer ISI evokes a larger P300 amplitude but increases the overall run time. Subjects with disabilities may find it difficult to stay focussed on stimulus for a longer period and hence may lead to a decrease in accuracy rate as well as amplitude.

Information transfer rate (ITR) is a general assessment metric developed for BCI systems that specifies how much information is transmitted by the output of a device. It is a standard measure of the BCI systems that take into account the classification accuracy, the set of possible choices, and

the time taken for each selection (Wolpaw et al. 2002). In general, the ITR of P300 based system is low but the proposed study provides the improved result. To improve the ITR of the BCI system, many efforts have been made in the recent past; reducing the span of each trial and hence increasing the bit-rate, use of different signal processing techniques, and machine learning algorithms (Jin et al. 2011). This study evaluated these effects on BCI performance based on ITR and found that smaller ISI provides better results as overall run time decreases while the machine learning algorithm (QDA) has shown better results than the most frequently used techniques.

To evaluate the performance of the authentication system, the commonly used matrices are FAR, FRR, EER, ROC, sensitivity, and specificity. In recent times, a lot of emphases are given on FAR as it determines the probability of incorrectly accepted unauthorized use by the system. On the other hand, FRR determines the probability of incorrectly rejected authorized users by the system (Araújo et al. 2005). For a reliable authentication system, excess of either of these conditions is unacceptable. A false acceptance rate (FAR) is worse than a false rejection rate (FRR), as most clients tend to reject genuine users rather than accept fraudsters. Therefore, a reliable authentication system must have a balance between the two error rates. The current study achieves low FAR (2.77%) corresponding to acceptable FRR (3.21%). For the proposed security system, classification results provide mean sensitivity equals 0.972 which indicates that the system identified 97.2% genuine user correctly while mean specificity equals 0.968 that indicates the system recognized 96.8% of the unauthenticated user correctly (Shakil et al. 2020). As discussed earlier, the Equal Error Rate (EER), which is a point where FAR and FRR are identical, is implemented to measure the effectiveness of the systems. For better performance of the authentication systems, it is desirable to have lower EER (Pham 2016). The proposed method in the present study achieves EER of 2.86% and 3.11%. Classification model performance can also be assessed by the ROC curve and the AUC. ROC plot depends on two fundamental evaluation metrics i.e. specificity and sensitivity. It plots TPR (sensitivity) against FPR ( $1 - \text{specificity}$ ). It can also be used to compare the performance of multiple users i.e. if the ROC curve of one user is entirely enveloped by the other user's curve then the latter's performance is considered superior. The ROC curve obtained from the current study reveals that subject 8 acquired the highest classification accuracy while subject 3 acquired the least amongst the three of them. Another performance parameter used in this study is an area under the ROC curve (AUC). It determines the capability of the system to differentiate between two classes. Theoretically, it ranges between 0 to

1. That means, higher the AUC, better the system is at differentiating between the genuine user and an imposter.

In any proposed security model, precision determines how accurately a particular class (target or non-target) has been predicted. The proposed model achieves mean precision (96.7%) indicating that all predicted scores belong to a particular class only. The current study achieves mean F1-score equals to 96.9%. A reliable security system achieves the highest F1 score value of 1.

The results show that the QDA algorithm achieved much better performance than the KNN and the QSVM algorithms in terms of not only classification accuracy but also bit rates. The performance comparison of three classifiers for ten subjects (S1 to S10) showed an  $F$ -test value of 125.483 and  $p < \alpha$ , hence we reject the null hypothesis and accept the alternative hypothesis that is, results obtained from three classifiers showed significant difference ( $\alpha = 0.05$ ) in terms of average accuracy. For ITR comparison, the value of the  $F$ -test was found to be 151.951 with  $p < \alpha$ , hence we reject the null hypothesis and accept the alternative hypothesis that is, results obtained from three classifiers showed significant difference ( $\alpha = 0.05$ ) in terms of ITR also.

Chen et al. (2016) proposed an EEG-based authentication framework that depends on ERPs that are evoked by a rapid serial visual presentation (RSVP) paradigm. In the RSVP based paradigm, pictures of different objects were introduced individually in a sequential way that means subjects need to focus their gaze only at one area located on a computer screen. The single-trial classification accuracy for the 28 and 16 channel wet electrode configurations was  $87.8 \pm 5.1\%$  and  $85.9 \pm 5.0\%$  respectively, and for the dry electrode setup, the average accuracy is  $78.2 \pm 5.7\%$  whereas, the average FAR is  $3.33 \times 10^{-5}$ . Yeom et al. (2013) proposed a paradigm in which self-face and non-self-face pictures are used as stimuli, where verification is done by comparing his/her observed biometric with that of the stored database. Here, self-face indicates the subject's face picture (target), whereas non-self-face indicates pictures of random people (non-target). The proposed method produced an average accuracy of 85.5%, FAR of 14.5%, and FRR of 14.5%. Mu et al. (2016) proposed a paradigm based on self-photos and non-self-photos similar to the study discussed by Yeom et al. The significant differences between these two paradigms were in terms of reduction in display time, feature extraction technique (fuzzy entropy instead of temporal features) and feature classification technique (Back Propagation instead of Gaussian Support Vector Machine). The classification accuracy obtained from the paradigm was 87.3%, whereas FAR and FRR were 5.5% and 5.6% respectively. Wu et al. (2018) proposed the EEG based authentication system in which the users were asked to concentrate on the face

based RSVP stimulus, and EEG attributes were stored in the database to be used at the time of login. The result showed a mean accuracy of 91.46% and the FAR of 9.23% and FRR of 7.85%.

Table 1 shows the approach based performance comparison of the current study with that of previous works. The quality comparison shows the superiority of our proposed method in terms of overall classification accuracy of 97%, ITR (37.14 bits/min), FRR (3.21%), and FAR (2.27%).

## Conclusion

This paper suggested a novel P300-based authentication paradigm using the pictures of different objects as stimuli to evoke ERPs in a human brain. Since the uniqueness of the brain signals of an individual are strong when he/she is exposed to the visual stimulus. Therefore, it has been verified that the proposed simulation framework generates one of a kind of subject-explicit mind wave patterns when exposed to different objects pictured. It is evident from the results that the essential factors in optimizing the performance of the P300 classifier are, the matrix size, visual stimulus, flash duration, multiple session recording, and inter-stimulus interval. The current study showed that the overall results of accuracy and ITR are promising with a proposed paradigm condition. Thus, one has to consider these factors while developing a P300 speller based paradigm. Further, the performance of the three classification algorithms is tested using the same stimulus but in four different sessions, and the same fivefold cross-validation method has opted across each experiment session for each algorithm. It is clear from the performance results that the QDA classifier performed better than the other two classifiers in terms of accuracy, ITR, and computational time. Also, results show no significant classification differences across the sessions, therefore, it can be concluded that the P300 response remains effective over a long period.

Although the proposed authentication scheme is slow as compared to traditionally used biometric methods, it does have an advantage over them because it cannot be mimicked or faked and can also be used by disabled users with substantial brain functioning. The current work was conducted using healthy participants, and the results obtained were based on their performance. The study can also be applied to subjects with impairments, such as disabled patients, to compare their performance with healthy subjects. Furthermore, the effect of various emotional states (happy, sad, and angry, etc.) on authentication results can also be explored as the EEG of individuals may vary if stress signals are present. This work can be extended by comparing different electrode configurations in



combination with different visual or auditory stimuli. Since the EEG-based authentication system are hard to manipulate or forge and it cannot be lost by users therefore EEG has great potential for use in applications for individual recognition. However, processing speed, classification accuracy, and user-friendly prototypes need to develop before commercial EEG-based human recognition systems are feasible. It is evident from the presented results that the changes made in the visual stimuli are reflected in the classification performances obtained. Therefore, the proposed method can be a promising approach to enhance the BCI device performance and can be an efficient method in BCI based authentication system design.

Furthermore, most BCI based authentication systems are at the testing stage and efforts have been taken to integrate them into the lives of people for continuous use. Existing BCI systems are uncomfortable because the electrodes have to be moistened, and the electrode connections require regular adjustment. But, recent portable devices with a limited number of dry electrodes provide a good solution for existing EEG based authentication systems. Also, these systems can be introduced to devices like desktops, tablets, and mobile phones by developing an on-site application that can guarantee privacy. Taking into account the development of artificial intelligence chips, the cost of processing equipment continues to decline. Therefore, these systems can also be introduced in organizations where high-end protection is required for information security in the near future.

**Abbreviations** BCI: Brain–computer interface; SSVEP: Steady-state visual evoked potential; ERD, EEG: Electroencephalogram; FAR: False rejection rate; FRR: False acceptance rate; ITR: Information transfer rate; ERP: Event-related potential; QDA: Quadratic discriminant analysis

**Acknowledgements** The authors would like to thank the subjects for participating in this experiment.

**Funding** This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

## Compliance with ethical standards

**Conflict of interest** The authors declare that they have no competing interests.

**Ethics approval and consent to participate** Experiments on human subjects had conducted with the ethical approval of the ethics committee of the institute.

## References

Abbas SN, Abo-Zahhad M (2017) Eye blinking EOG signals as biometrics. In: Jiang R, Al-maadeed S, Bouridane A, Crookes P,

- Beghdadi A (eds) Biometric security and privacy. Signal processing for security technologies. Springer, Cham, pp 121–140. [https://doi.org/10.1007/978-3-319-47301-7\\_5](https://doi.org/10.1007/978-3-319-47301-7_5)
- Ahirwal MK, Londhe ND (2012) Power spectrum analysis of EEG signals for estimating visual attention. *Int J Comput Appl* 42:22–25
- Allison BZ, Pineda JA (2003) ERPs evoked by different matrix sizes: implications for a brain computer interface (BCI) system. *IEEE Trans neural Syst Rehabil Eng* 11:110–113
- Araujo LCF, Sucupira LHR, Lizarraga MG et al (2005) User authentication through typing biometrics features. *IEEE Trans signal Process* 53:851–855
- Arslan B, Yorulmaz E, Akca B, Sagioglu S (2016) Security perspective of biometric recognition and machine learning techniques. In: 2016 15th IEEE international conference on machine learning and applications (ICMLA). IEEE, pp 492–497
- Artzi NS, Shriki O (2018) An analysis of the accuracy of the P300 BCI. *Brain-Computer Interfaces* 5:112–120
- Bhattacharyya D, Ranjan R, Alisherov F, Choi M (2009) Biometric authentication: a review. *Int J u-and e-Serv Sci Technol* 2:13–28
- Blocki J, Komanduri S, Procaccia A, Sheffet O (2013) Optimizing password composition policies. In: Proceedings of the fourteenth ACM conference on Electronic commerce. ACM, pp 105–122
- Burges CJC (1998) A tutorial on support vector machines for pattern recognition. *Data Min Knowl Discov* 2:121–167
- Cecotti H (2011) Spelling with non-invasive brain–computer interfaces—current and future trends. *J Physiol* 105:106–114
- Chen Y, Atnafu AD, Schlattner I et al (2016) A high-security EEG-based login system with RSVP stimuli and dry electrodes. *IEEE Trans Inf Forensics Secur* 11:2635–2647
- Cheng J-M, Wang H-C (2004) A method of estimating the equal error rate for automatic speaker verification. In: 2004 International symposium on Chinese spoken language processing. IEEE, pp 285–288
- Donchin E, Spencer KM, Wijesinghe R (2000) The mental prosthesis: assessing the speed of a P300-based brain–computer interface. *IEEE Trans Rehabil Eng* 8:174–179
- Duda RO, Hart PE, Stork DG (2001) Pattern classification. Wiley, New York, p 680
- El Saddik A, Orozco M, Asfaw Y et al (2007) A novel biometric system for identification and verification of haptic users. *IEEE Trans Instrum Meas* 56:895–906
- Farwell LA, Donchin E (1988) Talking off the top of your head: toward a mental prosthesis utilizing event-related brain potentials. *Electroencephalogr Clin Neurophysiol* 70:510–523
- Fawcett T (2006) An introduction to ROC analysis. *Pattern Recognit Lett* 27:861–874
- Fazel-Rezai R, Abhari K (2009) A region-based P300 speller for brain–computer interface. *Can J Electr Comput Eng* 34:81–85
- Forget A, Chiasson S, Van Oorschot PC, Biddle R (2008) Improving text passwords through persuasion. In: Proceedings of the 4th symposium on usable privacy and security. ACM, pp 1–12
- Guan C, Thulasidas M, Wu J (2004) High performance P300 speller for brain–computer interface. In: IEEE International workshop on biomedical circuits and systems, 2004. IEEE, pp S3–S5
- Guo F, Hong B, Gao X, Gao S (2008) A brain–computer interface using motion-onset visual evoked potential. *J Neural Eng* 5:477
- Han J, Kamber M, Pei J (2012) Data mining: concepts and techniques, vol 10. Morgan Kaufman Publishers, Waltham, 978–1 pp
- Henson RN, Goshen-Gottstein Y, Ganel T et al (2003) Electrophysiological and haemodynamic correlates of face perception, recognition and priming. *Cereb Cortex* 13:793–805
- Hitchcock DC (2003) Evaluation and combination of biometric authentication systems. Dissertation, University of Canberra
- Ille N, Berg P, Scherg M (2002) Artifact correction of the ongoing EEG using spatial filters based on artifact and brain signal



- topographies. *Clin Neurophysiol* 19:113–124. <https://doi.org/10.1097/00004691-200203000-00002>
- Jain A, Ross A, Prabhakar S (2004) An introduction to biometric recognition. *Circuits Syst Video Technol IEEE Trans* 14:4–20. <https://doi.org/10.1109/TCSVT.2003.818349>
- Jin J, Allison BZ, Sellers EW et al (2011) An adaptive P300-based control system. *J Neural Eng* 8:36006
- Kaongoen N, Yu M, Jo S (2017) Two-factor authentication system using P300 response to a sequence of human photographs. *IEEE Trans Syst Man Cybern Syst* 50:1178–1185
- Kaufmann T, Schulz SM, Grünzinger C, Kübler A (2011) Flashing characters with famous faces improves ERP-based brain–computer interface performance. *J Neural Eng* 8:56016
- Kayikcioglu T, Aydemir O (2010) A polynomial fitting and k-NN based approach for improving classification of motor imagery BCI data. *Pattern Recognit Lett* 31:1207–1215
- Kellicut-Jones MR, Sellers EW (2018) P300 brain-computer interface: comparing faces to size matched non-face stimuli. *Brain-Computer Interfaces* 5:30–39
- Kosti MV, Georgiadis K, Adamos DA et al (2018) Towards an affordable brain computer interface for the assessment of programmers’ mental workload. *Int J Hum Comput Stud* 115:52–66
- Kwong KK, Belliveau JW, Chesler DA et al (1992) Dynamic magnetic resonance imaging of human brain activity during primary sensory stimulation. *Proc Natl Acad Sci* 89:5675–5679
- Lashkari AH, Saleh R, Towhidi F, Farmand S (2009) A complete comparison on pure and cued recall-based graphical user authentication algorithms. In: 2009 Second international conference on computer and electrical engineering. IEEE, pp 527–532
- Liarokapis F, Debattista K, Vourvopoulos A et al (2014) Comparing interaction techniques for serious games through brain–computer interfaces: a user perception evaluation study. *Entertain Comput* 5:391–399
- Lin Z, Zhang C, Wu W, Gao X (2006) Frequency recognition based on canonical correlation analysis for SSVEP-based BCIs. *IEEE Trans Biomed Eng* 53:2610–2614
- Lu J, Speier W, Hu X, Pouratian N (2013) The effects of stimulus timing features on P300 speller performance. *Clin Neurophysiol* 124:306–314
- Marcel S, Millán JdR (2007) Person authentication using brainwaves (EEG) and maximum a posteriori model adaptation. *IEEE Trans Pattern Anal Mach Intell* 29:743–752
- Martens SMM, Hill NJ, Farquhar J, Schölkopf B (2009) Overlap and refractory effects in a brain–computer interface speller based on the visual P300 event-related potential. *J Neural Eng* 6:26003
- McFarland DJ, Sarnacki WA, Townsend G et al (2011) The P300-based brain–computer interface (BCI): effects of stimulus rate. *Clin Neurophysiol* 122:731–737
- Meinicke P, Kaper M, Hoppe F et al (2002) Improving transfer rates in brain computer interface: a case study. In: *Neural information processing systems*, pp 1107–1114
- Mu Z, Hu J, Min J (2016) EEG-based person authentication using a fuzzy entropy-related approach with two electrodes. *Entropy* 18:432. <https://doi.org/10.3390/e18120432>
- Narkhede S (2018) Understanding AUC-ROC curve. *Toward Data Sci* 26
- Nicolas-Alonso LF, Gomez-Gil J (2012) Brain computer interfaces, a review. *Sensors* 12:1211–1279
- Oweis RJ, Hamdi N, Ghazali A, Lwissy K (2013) A comparison study on machine learning algorithms utilized in P300-based BCI. *J Heal Med Inform* 4:2
- Palaniappan R (2008) Two-stage biometric authentication method using thought activity brain waves. *Int J Neural Syst* 18:59–66
- Pan J, Li Y, Gu Z, Yu Z (2013) A comparison study of two P300 speller paradigms for brain–computer interface. *Cogn Neurodyn* 7:523–529
- Paranjape RB, Mahovsky J, Benedicenti L, Koles Z (2001) The electroencephalogram as a biometric. In: *Canadian conference on electrical and computer engineering 2001. Conference proceedings (Cat. No. 01TH8555)*. IEEE, pp 1363–1366
- Pham TD (2016) EEG-based person authentication for security systems. Doctoral dissertation, University of Canberra
- Pham T, Ma W, Tran D, et al (2014) Multi-factor EEG-based user authentication. In: 2014 International joint conference on neural networks (IJCNN). IEEE, pp 4029–4034
- Picton TW (1992) The P300 wave of the human event-related potential. *J Clin Neurophysiol* 9:456–479
- Posner MI, Petersen SE (1990) The attention system of the human brain. *Annu Rev Neurosci* 13:25–42
- Raju AS, Udayashankara V (2018) A survey on unimodal, multi-modal biometrics and its fusion techniques. *Int J Eng Technol* 7:689–695
- Rak RJ, Kołodziej M, Majkowski A (2012) Brain–computer interface as measurement and control system the review paper. *Metrol Meas Syst* 19:427–444
- Ramadan RA, Vasilakos AV (2017) Brain computer interface: control signals review. *Neurocomputing* 223:26–44
- Salvaris M, Sepulveda F (2009) Visual modifications on the P300 speller BCI paradigm. *J Neural Eng* 6:46011
- Schomaker L (2007) Advances in writer identification and verification. In: *Ninth international conference on document analysis and recognition (ICDAR 2007)*. IEEE, pp 1268–1273
- Sellers EW, Krusienski DJ, McFarland DJ et al (2006) A P300 event-related potential brain–computer interface (BCI): the effects of matrix size and inter stimulus interval on performance. *Biol Psychol* 73:242–252
- Serby H, Yom-Tov E, Inbar GF (2005) An improved P300-based brain–computer interface. *IEEE Trans neural Syst Rehabil Eng* 13:89–98
- Shakil KA, Zareen FJ, Alam M, Jabin S (2020) BAMHealthCloud: a biometric authentication and data management system for healthcare data in cloud. *J King Saud Univ Inf Sci* 32:57–64
- Shashibala T, Gawali BW (2016) Brain computer interface applications and classification techniques. *Int J Eng Comput Sci* 5:17260–17267
- Snodgrass JG, Vanderwart M (1980) A standardized set of 260 pictures: norms for name agreement, image agreement, familiarity, and visual complexity. *J Exp Psychol Hum Learn Mem* 6:174
- Souza DFL, Burlamaqui AMF, Souza Filho GL (2017) A multi factor authentication approach based on biometrics, optical interference and chaotic maps. *IEEE Lat Am Trans* 15:1700–1708
- Streiner DL, Cairney J (2007) What’s under the ROC? An introduction to receiver operating characteristics curves. *Can J Psychiatry* 52:121–128
- Thorpe J, Van Oorschot PC, Somayaji A (2005) Pass-thoughts: authenticating with our minds. In: *Proceedings of the 2005 workshop on new security paradigms*. ACM, pp 45–56
- Vaughan TM, Heetderks WJ, Trejo LJ, et al (2003) Brain–computer interface technology: a review of the second international meeting
- Wolpaw JR, Birbaumer N, McFarland DJ et al (2002) Brain–computer interfaces for communication and control. *Clin Neurophysiol* 113:767–791
- Wu Q, Yan B, Zeng Y et al (2018) Anti-deception: reliable EEG-based biometrics with real-time capability from the neural response of face rapid serial visual presentation. *Biomed Eng Online* 17:55

- Yeom S-K, Suk H-I, Lee S-W (2013) EEG-based person authentication using face stimuli. In: 2013 International winter workshop on brain–computer interface (BCI). IEEE, pp 58–61
- Zeynali M, Seyedarabi H (2019) EEG-based single-channel authentication systems with optimum electrode placement for different mental activities. *Biomed J* 42:261–267
- Zhang Y, Zhao Q, Jin J et al (2012) A novel BCI based on ERP components sensitive to configural processing of human faces. *J Neural Eng* 9:26018

**Publisher's Note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.